ESCUELA SUPERIOR POLITÉCNICA DEL CHIMBORAZO

MECANISMOS PARA MITIGAR RIESGOS GENERADOS POR LA INTRUSIÓN EN ROUTERS DE FRONTERA BASADOS EN RESULTADOS DE UN HONEYPOT VIRTUAL

LUIS FABIAN HURTADO VARGAS

Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo, presentado ante el Instituto de Posgrado y Educación Continua de la ESPOCH, como requisito parcial para la obtención del grado de MAGISTER EN SEGURIDAD TELEMÁTICA

RIOBAMBA - ECUADOR

JUNIO – 2017

ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

CERTIFICACIÓN:

EL TRIBUNAL DE TRABAJO DE TITULACIÓN CERTIFICA QUE:

El **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** titulado "MECANISMOS PARA MITIGAR RIESGOS GENERADOS POR LA INTRUSIÓN EN ROUTERS DE FRONTERA BASADOS EN RESULTADOS DE UN HONEYPOT VIRTUAL", de responsabilidad del Ing. Luis Fabián Hurtado Vargas, ha sido prolijamente revisado y se autoriza su presentación.

Tribunal:

Ph.D. Fredy Bladimir Proaño Ortiz **PRESIDENTE**	**FIRMA**
Ing. Marco Vinicio Ramos Valencia, M.Sc. **DIRECTOR**	**FIRMA**
Ing. Diego Fernando Ávila Pesantez, M. Sc. **MIEMBRO**	**FIRMA**
Ing. Ruth Genoveva Barba, M. Sc. **MIEMBRO**	**FIRMA**

Riobamba, Junio 2017

DERECHOS INTELECTUALES

Yo, Luis Fabián Hurtado Vargas, declaro que soy responsable de las ideas, doctrinas y resultados expuestos en el **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo**, y que el patrimonio intelectual generado por la misma pertenece exclusivamente a la Escuela Superior Politécnica de Chimborazo.

_____

Luis Fabián Hurtado Vargas
No. Cédula: 0913563326

DECLARACION DE AUTENTICIDAD

Yo, Luis Fabián Hurtado Vargas, declaro que el presente **Trabajo de Titulación modalidad Proyectos de Investigación y Desarrollo,** es de mi autoría y que los resultados del mismo son auténticos y originales. Los textos constantes en el documento que provienen de otra fuente están debidamente citados y referenciados.

Como autor, asumo la responsabilidad legal y académica de los contenidos de este proyecto de investigación de maestría.

Riobamba, junio de 2017

_____

Luis Fabián Hurtado Vargas
No. Cédula: 0913563326

DEDICATORIA

Agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida.

Al concluir este presente trabajo es menester una dedicatoria a mis padres, LUIS ALBERTO E INES MARIA que siempre me apoyaron desinteresadamente en toda mi etapa estudiantil y vida.

A mis hermanos KATIUSHKA Y JULIO CESAR, por haber compartido conmigo muchos días de juegos y enseñanza.

A mi esposa KAREN MARLENE, la única mujer con la que podía casarme y llevar adelante nuestro proyecto de vida, por ser la mujer ideal, por mi apoyo incondicional y por demostrarme la gran fe que tiene en mí.

Y una dedicatoria especial a mis hijas FABIANNA ABIGAIL y LUCIANNA VALENTINA, ya que Fabiannita, desde que te saque de la barriga de tu mamita y te corte el cordón umbilical sentí que jamás en la vida nos íbamos a separar, por su amor incondicional demostrado día a día, por ser esa motivación de todo lo que hago, mi motivo principal para vivir y seguir siempre adelante, Luciannita, te amo simplemente desde el momento en que me entere que lo que estaba moviéndose y creciendo dentro de vientre de tu mamita era una hermosa niña con una personalidad y sonrisa hermosa y mi 3er motivo para no desmayar en la vida, ya que tu completas mi bendición celestial, y

Simplemente los amo.

Fabito!

AGRADECIMIENTO

Culminada esta etapa de formación académica, quiero expresar mi profundo agradecimiento a las autoridades de la Escuela Superior Politécnica de Chimborazo.

Mi gratitud imperecedera, de manera muy especial a Ing. Vinicio Ramos Valencia mi director de esta investigación y amigo por el valioso apoyo brindado durante el desarrollo del presente trabajo y a mi amigo personal Ing. Luis Alberto Pazmiño, por su soporte, dedicación en momentos de estudios, aclararme miles de dudas, y en los momentos de sano esparcimiento.

A todos los catedráticos del programa de maestría, que de una manera idónea, supieron orientarme en la construcción del conocimiento en los diferentes módulos disertados.

Al Ing. Diego Ávila, un amigo incondicional y excelente catedrático.

A todos ellos que Dios y la humanidad les recompensen por tan fructífera labor a favor de la educación.

CONTENIDO

INDICE DE TABLAS

INDICE DE FIGURAS

INDICE DE ANEXOS

RESUMEN

En la presente investigación se implementaron mecanismos para mitigar riesgos generados por la intrusión en Routers de frontera basados en resultados de un Honeypot Virtual. Se analizaron las principales vulnerabilidades y amenazas encontradas comúnmente en ambientes de red WAN, donde el dispositivo con mayor riesgo generado es el Router de Frontera o de Borde, específicamente en su protocolo SNMP. Para la construcción de la solución planteada, se analizó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información PAe - MAGERIT v.3, el paper de la revista científica IEEE Honeypot Router for routing protocols protection y el libro Honeypots tracking hackers, también se consideraron algunas recomendaciones de estándares y normas de seguridad en ambientes WAN. La solución llamada HONEYPOT-ROUTER-SNMP está enfocada en ataques como DDos, Rastreo de Puertos y Ataques de Fuerza Bruta, los cuales amenazan en gran porcentaje al impacto generado por el riesgo de seguridad del protocolo SNMP en sus 3 versiones; y consta de 2 componentes que son 1) Infraestructuras de solución (con 2 etapas a) Estudio y detección de vulnerabilidades y ataques, b) Aplicar la protección y medidas de seguridad) y 2) Mecanismos de Prevención (con los cuales se completan los pasos para la detección y prevención de amenazas). Mediante la solución propuesta se logró minimizar en un 95% las vulnerabilidades y riesgos que afectaban al buen funcionamiento del Router de Borde, con lo cual, se aumentó notablemente su disponibilidad y confiabilidad. Se recomienda la implementación de una solución de Administración de Correlación de Eventos después del IPS donde se emitirán alertas, las cuales deberán ser revisadas por el ente de seguridad designado por la organización.

Palabras clave: <TECNOLOGÍA Y CIENCIAS DE LA INGENIERÍA>, <INGENIERÍA EN TELECOMUNICACIONES>, <REDES>, SEGURIDAD TELEMÁTICA>, <HONEYPOT (HERRAMIENTA)>, <PROTOCOLO DE ENRUTAMIENTO>, <SISTEMA DE DETECCIÓN DE INTRUSOS (IDS)>, < SISTEMA DE PREVENCIÓN (IPS)>.

ABSTRACT

In the present investigation, the mechanisms to mitigate the risks generated by the intrusion in routers based on the results of a Virtual HoneyPot were implemented. The main vulnerabilities and threats were found commonly within network environments WAN, where the device with a bigger generated risk is the edge router, in its protocol SNMP specifically. For the construction of the planned solution, the Methodology of Analysis and the Risk Management of the Information Systems PAe-MAGERIT v.3 were analyzed, the scientific journal IEEE: "Honeypot Router for routing Protocol protection" and the book "Honeypots Tracking Hackers". In addition, some standard recommendations and safety norms in environments WAN. The solution called HONEYPOT-ROUTER-SNMP is focused on attacks such as: DDos, Tracking of Ports, and Brute Force Attacks, which threat in a big percentage the impact generated by the risk of safety SNMP within its three versions, and consists of two components which are: 1) Infrastructures of solution (with two stages: a) Study and Detection of vulnerabilities and attacks and b) Apply the protection and safety measurements); and 2) Prevention Mechanisms (with which the steps are completed to detect and prevent threats). By using the solution of functioning of the edge router, with which, its availability and trustworthy increased, notoriously. It is recommended the implementing of a solution of Management of Event Correlation after the IPS, where the alerts will be emitted, which should be verified and in consequence designated by the organization.

KEY WORDS: <TECHNOLOGY AND ENGINEERING SCIENCES>, <ENGINEERING IN TELECOMMUNICATIONS>, <NETWORKS>, <TELEMATICS SAFETY>, <HONEYPOT (TOOL) >, <ROUTING PROTOCOL>, <INTRUDER DETECTION SYSTEM (IDS) >, <INTRUDER PREVENTION SYSTEM (IPS) >.

CAPITULO I

1. INTRODUCCION

1.1. Problema de Investigación

1.1.1. Planteamiento del problema

"La seguridad del bien más preciado que tiene toda institución, la información", cada día sigue siendo vulnerada de muchas maneras, la delincuencia informática está en constante evolución y búsqueda de nuevas formas de obtener la misma sin ningún reparo y por cualquier vía. Una de esas vías de acceso a los datos de origen privado, son los equipos de frontera o que dan la cara hacia la Internet, como son los Routers o Enrutadores. Actualmente se están haciendo estudios para tratar de mitigar el riesgo de intrusión a través de los protocolos de enrutamiento en Routers de forma favorable sin disminuir el performance de los equipos. Se ha descubierto que estos protocolos no son los únicos que ofrecen vulnerabilidades, también se han encontrado en el protocolo SNMP.

Los atacantes informáticos día a día buscan nuevas vulnerabilidades en todo equipo o software que esté conectado hacia la "red de redes". Estos equipos muchas veces no son configurados con la prolijidad y exactitud del caso, por lo que dejan muchas puertas abiertas para que sean accedidos impunemente, dado el caso de que estos son la primera vía de acceso hacia redes exteriores, la información fluye con la confianza de que va a llegar a su destino final, sin importar los riesgos que esta corra. Una de estas puertas abiertas son los protocolos de comunicación, los cuales no están protegidos en su totalidad ya que cuentan con una estructuración de naturaleza humana y por ende incurren en fallas.

SNMP (Simple Network Management Protocol) es un protocolo estándar más utilizados para la administración de red en Internet. Prácticamente todos los sistemas operativos, routers, switches, módems cable o ADSL modem, firewalls, etc. se ofrecen con el servicio SNMP.

Facilita el intercambio de información de administración entre dispositivos de red y permite a los administradores supervisar, buscar y resolver posibles problemas que aparezcan en la red.

Un grupo de investigación de la Universidad de Oulu, Finlandia, que estudia evalúa, desarrolla métodos de implementación, aplicaciones de prueba y software en general a fin de prevenir, descubrir y eliminar vulnerabilidades de seguridad en niveles de implementación, y ha desarrollado una suite de aplicaciones bajo el nombre de PROTOS (Oulu, U, 2010), diseñada para enviar cientos de pruebas a los demonios SNMP desde un sistema remoto con el objetivo de descubrir fallos de configuración o vulnerabilidades explotables. Esta herramienta tiene la capacidad de provocar la caída de demonios SNMP y dispositivos de hardware con SNMP.

QUE SE HA HECHO Y QUE NO SE HA HECHO A NIVEL GLOBAL Y NACIONAL

Actualmente se han hecho varias investigaciones sobre seguridad de protocolos en equipos routers, entre las cuales tenemos:

- **En lo referente al protocolo de enrutamiento RIP,** B.R. Smith, S. Murthy, y J.J. García-Luna-Aceves en 2011, describieron un esquema para asegurar protocolos de enrutamiento por vector distancia mediante el uso de la información del predecesor (Smith, R., Murthy, S., Garcia-Luna-Aceves, J., 2011)**.** En otro trabajo propuesto en 2006, se propusieron varios mecanismos eficientes utilizando un solo sentido hash de cadenas y árboles de autenticación para asegurar los protocolos de enrutamiento de vector de distancia (Hu, Y., Perrig, A., Johnson, D., 2006). Investigaciones en 2008, desarrollaron un método de detección de intrusión llamado método basado en sensores. Su técnica se basa en la topología de la red para generar automáticamente las firmas utilizadas por sensores para detectar ataques de enrutamiento (Mittal,V. & Vigna, G., 2008).

- **En lo referente al protocolo de enrutamiento OSPF,** trabajos realizados en 2006 proponen un enfoque preventivo usando criptografía, específicamente, firmas digitales para proteger la integridad de las LSA (Avisos Link-State) (Murphy, S. L., & Badger, M. R., 2006). Otro trabajo de investigación en 2010 se provee un sistema de detección de intrusiones en tiempo real llamado JiNao para supervisar el estado de los protocolos de enrutamiento de estado de enlace como OSPF (Chang, H., Wu, S., Jou, Y., 2010). JiNao utiliza máquinas de estados finitos para detectar ataques dirigidos a este protocolo.

- **En lo referente al protocolo de enrutamiento BGP para Routers de frontera,** investigadores en el 2010, propones el uso de PKI centralizado para la autenticación de los números AS y la propiedad de los prefijo IP (Kent, S., Lynn, C., & Seo, K., 2010). Un grupo de investigadores de Cisco Systems propusieron en el 2004 validar la exactitud y autorización de los datos transportados dentro de BGP, y también para prevenir el anuncio de los prefijos no autorizadas(Cisco Systems, 2004) . Otra mejora de BGP llamada psBGP (Pretty Secure BGP) fue propuesto por Evangelos Kranakis (Evangelos Kranakis, 2010).

Otro trabajo fue el software HONEYD el cual hace las veces de un Router Cisco, pero le falta algo, características básicas como la emulación de protocolos de enrutamiento. Además, HONEYD es un honeypot de baja interacción, por lo que no puede actuar fuertemente con el atacante, lo cual impidió recolectar mucha información sobre ataques de enrutamiento. Para reforzar la seguridad de los protocolos en dispositivos routers, se necesitó un enfoque adicional capaz de detectar nuevos ataques y comprender las técnicas y los métodos utilizados por los atacantes informáticos.

La idea del autor, conllevó a utilizar un honeypot como una solución complementaria a herramientas de seguridad existente. De hecho, los honeypots han demostrado su eficacia en la detección de nuevos ataques (ataque 0-day), gracias a que constantemente se está analizando en tráfico de la red (Spitzner, L, 2016). Sin embargo, como ya se ha mencionado hay una falta en el despliegue de honeypots con funciones de routers para analizar protocolos de administración de red.

El objetivo conllevó a disminuir las vulnerabilidades que presenta el protocolo SNMP a través de una inyección de código malicioso para acceder directamente al router o al terminal de un administrador cuando el mismo intenta loguearse en el. Por lo que el enfoque de la presente investigación se diferenció de las investigaciones anteriores las cuales se orientaban a proponer soluciones de seguridad dirigidas solo a protocolos de enrutamiento, ponemos a consideración el despliegue de un HONEYPOT ROUTER-SNMP para estudiar, investigar y detectar los ataques contra los protocolos de Administración de Red y así mejorar la seguridad.

Este tipo de Honeypot es una idea nueva que pretende ser útil para el análisis de vulnerabilidades no solo de protocolos Administración de Red, sino, de protocolos los cuales no cuenten con refuerzos de seguridad.

1.2. FORMULACIÓN DEL PROBLEMA

Se mitigarán los riesgos de seguridad asociados a Routers de Frontera utilizando los resultados de los estudios generados por equipos señuelo, como un Honeypot Router

1.2.1 SISTEMATIZACIÓN DEL PROBLEMA

¿Cuáles son las tecnologías existentes para atraer a atacantes informáticos?
¿Cuáles son las consecuencias de no tener aplicadas las configuraciones de seguridad en los routers de frontera?
¿Cuáles son los ataques más comunes realizados a routers de frontera por el protocolo SNMP?
¿Cómo se podrían diagnosticar el nivel de riesgo e impacto en los routers de frontera?
¿Cuáles son las mejores prácticas para fortalecer la seguridad en routers de frontera?

1.3. JUSTIFICACION

1.3.1. Justificación teórica

Abdallah Ghourabi, Tarek Abbes y Adel Bouhoula en su paper "Honeypot Router for routing protocols" (Ghourabi, A., Abbes, T., Bouhoula, A., 2010), indican que un honeypot es un sistema informático voluntariamente vulnerable a uno o más amenazas conocidas, destinadas a atraer a los atacantes informáticos para explorar sus estrategias de ataque. Las diferentes acciones que van a realizar los atacantes serán ingresadas en un registro diario (LOGS) y se analizarán para entender las estrategias seguidas por los hackers para lograr su fin.

La idea atrás de la tecnología de los honeypots es mostrar a los atacantes informáticos un sistema virtual que parezca el sistema real, cuya intención es atraer (como la miel) a los atacantes simulando ser sistemas débiles o con fallas de seguridad, evidentes, o no del todo, pero si lo suficiente para atraerlos y ser un reto para sus habilidades de intrusión, de esa manera los ataques se efectuarán sobre ese sistema sin causar ningún daño al sistema real (Pazmiño, L., 2011), lo cual es sumamente beneficio para los analistas de seguridad y administradores de red, ya que aprenden nuevas técnicas, herramientas y motivaciones de los atacantes y así protegen mejor a los sistemas de producción. Si bien existen trabajos que abordan la temática de los

Honeypots, no hay muchos que se centren en el desarrollo de Honeypots que hagan la tarea de equipos de frontera, menos aún que adicional realicen estadísticas de los puertos más atacados o que se interesen en un protocolo en particular.

Este trabajo de investigación se centró en establecer escenarios de pruebas y propuestas de solución donde, se puedan estudiar minuciosamente la vulnerabilidades que generen riesgos a la seguridad en Routers de Frontera a través del Protocolo Simple de Administración de Red, valiéndonos de la ayuda de un equipo señuelo para atraer a atacantes informáticos llamado Honeypot de tipo virtual y a la vez, aplicar las medidas de seguridad necesarias para disminuir el alto impacto de afectación generados en el mismo.

Como valor agregado a esta investigación, se generarán estadísticas de los ataques efectuados a las vulnerabilidades del protocolo simple de gestión de red SNMP ya que en la mayoría de equipos de alto riesgo en la Red WAN como los Routers de Frontera. Este protocolo viene habilitado por default con la cadena "public" para acceso de solo lectura y "private" (George Cybenko, 2012) para acceso de lectura y escritura, las cuales son transportadas a través de la red en "texto plano" por lo que no existe un nivel de seguridad adecuado y ser presa tranquilamente de un segundo ataque de negación de servicio dando paso la inestabilidad a gran escala en la red o su corte definitivo.

Las vulnerabilidades que se trató en esta investigación son las siguientes:

Manejo de Trampa (Trap handling): Múltiples vulnerabilidades fueron encontradas en numerosos decodificares NMSs y el proceso de capturas de mensajes SNMP(George Cybenko, 2012).

Gestión de peticiones (Request handling): La prueba también reveló debilidades en la forma en que muchos agentes SNMP decodifican y procesos de solicitud de mensajes SNMP(George Cybenko, 2012).

Estas vulnerabilidades resultaron del control insuficiente de los mensajes SNMP tanto como fueron recibidos y procesados por un sistema afectado. Para productos de diferentes marcas, estas vulnerabilidades pueden permitir ataques de fuerza bruta, DOS ataques de negación de servicio, vulnerabilidades de cadena de formato, obtención de múltiples datos GET BULK y desbordamiento de buffer (buffer overflow)(George Cybenko, 2012).

Las técnicas estudiadas quedaron a disposición de administradores de todos los niveles con necesidades de asegurar sus sistemas. Así como, documentación que permita a estos poder hacer un uso con conocimiento de causa de las técnicas para fortalecer sus equipos. Consideramos que el proyecto tiene un valor social ya que mediante la aplicación de sencillas técnicas de seguridad y utilizando Software Libre se podrá lograr alta disponibilidad y evitar caídas de servicio innecesarias que afecten a los interesados.

Es un aporte que beneficia a la industria, ya que, a través de una correcta lectura y aplicación adecuada de las técnicas aquí estudiadas, se puede mitigar o eliminar el impacto de ataques contra los equipos críticos de redes de las empresas para lo cual, se hizo uso de herramientas en Software Libre por la flexibilidad que ofrece de evolucionar rápidamente, integración y facilidades de estudio de estos procesos.

1.3.2. Justificación práctica

El campo / ambiente de comprobación y pruebas de la presente investigación será el laboratorio CISCO de la Escuela Superior Politécnica del Chimborazo, la cual generó la idea de todo el ámbito de acción de los atacantes informáticos tales como:

¿En Routers de Frontera, cual es el punto ciego por donde los atacantes están ingresando con mayor facilidad en los últimos años y no ha sido tomado en cuenta en la seguridad?
¿Cuáles son las técnicas de ataque utilizadas con más frecuencia?
¿Cuál es el objetivo común de los atacantes informáticos cada vez que realizan los intentos de intrusión?

1.4. OBJETIVOS DE LA INVESTIGACION

1.4.1. General

Proponer los mecanismos para mitigar riesgos asociados a la intrusión en routers de frontera basados en los resultados de una honeypot virtual.

1.4.2. Específicos

3. Estudiar los riesgos y vulnerabilidades de seguridad asociados al protocolo SNMP en Routers de Frontera.

4. Diseñar propuestas de solución, donde sea posible validar el porcentaje de afectación y mitigación de riesgos de seguridad asociados a la intrusión en Routers de Frontera por el protocolo SNMP.
5. Establecer escenarios de prueba para la puesta en marcha de los ataques que afecten al impacto de seguridad de Routers de Frontera, específicamente en el protocolo SNMP.
6. Aplicar reglas de seguridad en la infraestructura de solución propuesta.
7. Establecer las mejores recomendaciones que ayuden a fortalecer la seguridad en Routers de Frontera.

CAPITULO II

2. MARCO DE REFERENCIA

2.1. Routers

Según lo establecido por la empresa CISCO en su capacitación CCNA (Cisco Systems, 2010b), actualmente los routers poseen características de hardware y software muy superiores a las que tenían en su creación por la década de los 70, como por ejemplo el aumento de memoria RAM, la reducción de peso y temperatura, la codificación de datos por razones de seguridad y el encaminamiento de paquetes acelerado por lo que se encargan de dirigir los datos hacia otro router o un equipo computacional seleccionando la ruta más corta o adecuada, proceso que lo lleva a cabo por protocolos de enrutamiento los cuales se encuentran instalados dentro los routers.

Los Routers, son dispositivos que permiten la intercomunicación entre 2 o más subredes diferentes, por lo que pertenecen a la capa 3 del modelo OSI, para lo cual tienen la responsabilidad de cumplir con 2 procesos que son:

El proceso **Routing** se establece la mejor ruta o vía para que viajen los paquetes de datos desde el transmisor hasta el receptor, aquí es donde se crea la ya conocida tabla de enrutamiento, en cambio el proceso **Forwarding,** se encarga de enviar el paquete que ingresa por la interfaz de entrada a la de salida apropiada del enrutador. La ventaja de estos equipos es que generan tráfico de difusión o bradcast.

2.1.1 Clases de Enrutamiento

Las clases o tipos de enrutamiento fueron creados ya que para enviar los paquetes de datos entre dispositivos, se necesita establecer el mejor camino que recorrerá hasta llegar a cualquier host remoto. Dichos tipos o protocolos de enrutamiento, de forma independiente, pueden ejecutarse en un mismo enrutador, con el fin de ir actualizando las tablas de enrutamiento.

Existen 2 tipos de enrutamiento, que son estático y el dinámico, para su mejor comprensión los detallo en la siguiente tabla:

Tabla 1-2: Tipos de enrutamiento - Características

	Enrutamiento dinámico	**Enrutamiento estático**
Complejidad de configuración	Independiente del tamaño de la red	Se incrementa con el tamaño de la red
Conocimientos requeridos	Se requiere conocimiento avanzado	No se requieren conocimientos adicionales
Cambios de topología	Se adapta automáticamente a los cambios de la tecnología	Se requiere la intervención del administrador
Escalabilidad	Adecuado para topologías simples y complejas	Adecuado para topologías simples
Seguridad	Es menos seguro	Es más seguro
Uso de recursos	Utiliza CPU, memoria y ancho de banda	No se requieren recursos adicionales
Capacidad de predicción	La ruta depende de la topología actual	La ruta hacia el destino es siempre la misma.

Realizado por: Fabián Hurtado, 2016
Fuente: (Cisco Systems, 2010b)

2.1.2 Tipos de Routers

Los diferentes tipos de Routers están detallados en la siguiente tabla:

Tabla 2-2: Tipos de Routers - Características

Router SOHO	Utilizados mayormente en hogares.
Router Empresarial	Equipo robusto conecta muchos servicios.
Router de Acceso	Interconecta a clientes y sucursales.
Router de Distribución	Congregan tráfico de otros routers.
Router de Núcleo	Administran diversas topologías, columna vertebral que soporta conexiones de otros routers de acceso.

Realizado por: Fabián Hurtado, 2016
Fuente: (Cisco Systems, 2010b)

Routers de Frontera, borde o perimetral: Dispositivo el cual es tema de discusión del presente trabajo de investigación, son el punto de conexión entre varios sistemas autónomos o grupo de redes IP que tienen políticas de rutas propias e independientes, con otros sistemas autónomos o troncales de Internet. Poseen características exorbitantes en cuanto a hardware y software se refiere, manejando vario tipos de protocolos de enrutamiento. (Gerometa, O., 2011)

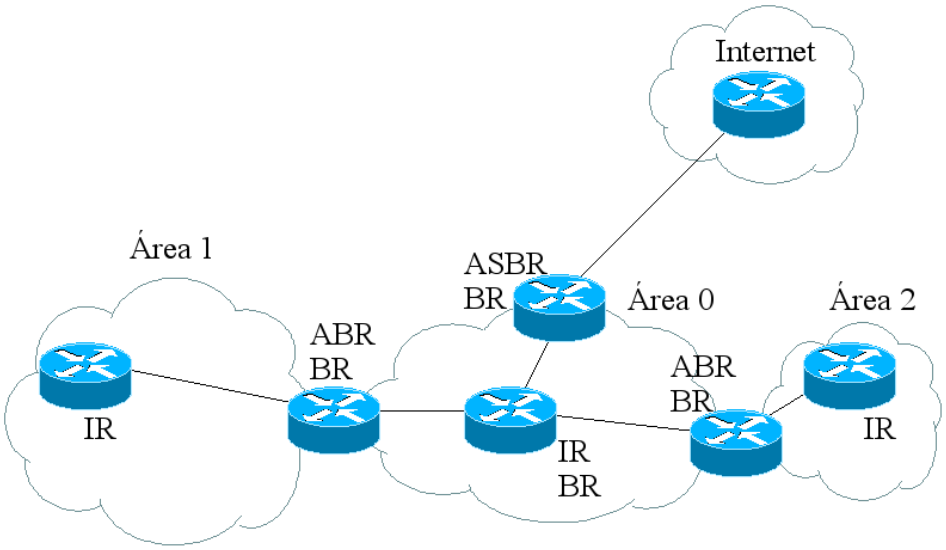


Figura 1-2: ABR-BR - Router de Borde, frontera o perimetral

Fuente: (Gerometa, O., 2011)

Son los encargados de enviar paquetes de datos de una red de confianza a varias redes no confiables recorriendo la gran avenida llamada Internet, en la cual se puede encontrar cualquier cantidad de amenazas como atacantes informáticos, los cuales pueden descubrir, violentar y explotar las vulnerabilidades de seguridad propias de este tipo de dispositivos.(Cisco Systems, 2010b)

Al ser este un tipo de router expuesto, significa que está conectado en un segmento fuera de firewalls empresariales o simplemente, que conectan una red segura con otra que no lo es, podrían no lograr finalizar sus objetivos trazados, pudiendo incapacitar a toda una organización u organizaciones de realizar negocios, por tal motivo, si estos dispositivos no ofrecen ningún tipo de seguridad o garantía no sólo serán incapaces de filtrar tráfico de red no deseado, sino que, también pueden ser blanco fácil para ataques de denegación de servicio, la cual llevaría a la red a un punto muerto.(Larios, A., Moreira, B., 2011)

Los routers de borde deben filtrar paquetes para que no caer en suplantación de direcciones IP, sin embargo, la posibilidad de que paquetes de origen malicioso penetren hacia la red interna o LAN puede ser muy alta y al no ser este router la última línea de defensa, la red corporativa podría quedar expuesta a cualquier ataque o siniestro de información.

2.1.3 Protocolos utilizados

El router de borde o frontera no deja de cumplir con su función principal que es el enrutamiento de paquetes de datos por la vía más adecuada utilizando protocolos de enrutamiento interiores, la única diferencia con los convencionales es que este dispositivo trabaja de forma expuesta, por lo consiguiente, utilizan protocolos de enrutamiento de tipo exterior, en esta sección se tratara el tema de cual protocolo es el ideal o el más utilizado ya que la arquitectura actual de internet así lo prioriza.

Los protocolos gateway interiores (IGP, Interior Gateway Protocols) se usan para intercambiar información de enrutamiento con un AS (Autonomous System) o una organización individual. Su objetivo es encontrar el mejor camino atravesando de la red interna, ejemplos de IGP son RIP, EIGRP y OSPF, por otro lado, los protocolos gateway exteriores (EGP, Exterior Gateway Protocols) funcionan en dispositivos que ubican el límite del AS, también se denominan gateways, routers de borde o de frontera y están diseñados para intercambiar información de enrutamiento entre los distintos sistemas autónomos, el cual sirve como traductor para asegurar que los datos de enrutamiento externos se interpreten exitosamente dentro de cada red de AS, el protocolo EGP más conocido y utilizado es BGP (Border Gateway Protocol).(Cisco Systems, 2016a)

Sistemas autónomos

Antes de explicar cómo trabaja el protocolo BGP, se explicará lo que son los AS. Un sistema autónomo (AS) es un conjunto de redes bajo el control administrativo de una única entidad que presenta una política de enrutamiento común para Internet. En la figura 2-2, las empresas A, B, C, D y E se encuentran todas bajo el control administrativo de un ISP (Proveedores de servicios de Internet) llamado ISP1. Entonces ISP1 presenta una política de enrutamiento común para todas estas empresas cuando publica rutas en ISP2. (Cisco Systems, 2006)

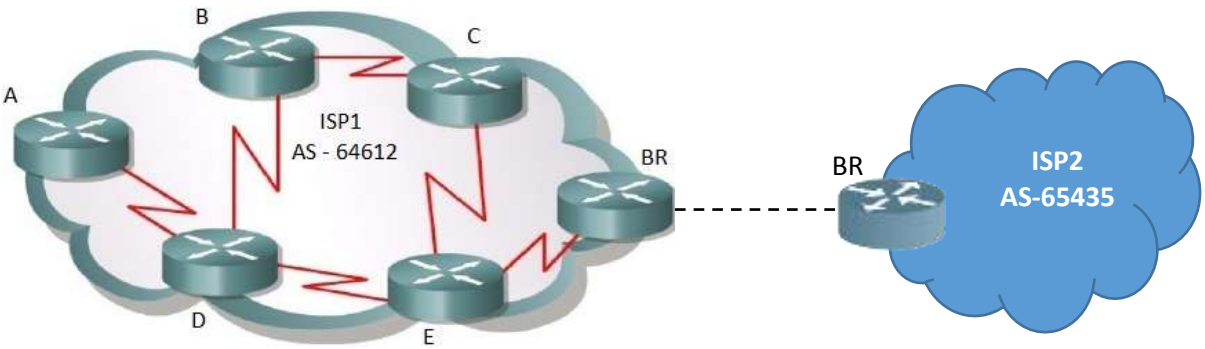


Figura 2-2: AS - Autonomous Systems
Fuente: (Cisco Systems, 2006)

Los lineamientos para la creación, selección y registro del sistema autónomo se describen en RFC 1930. La Autoridad de Números Asignados de Internet (IANA con sus siglas en inglés) asigna números AS, y es la misma autoridad que asigna el espacio de dirección IP. Por lo general los ISP, los proveedores de "backbone" de Internet y grandes instituciones que se conectan con otras entidades que también cuentan con un número de AS, los cuales son: Públicos: 1 – 49151, Privados: 64512 – 65534 los cuales nunca intercambian información con los públicos, y los Reservados: 0, del 49152 al 64511 y el 65535. (Cisco Systems, 2006)

Estos ISP y las grandes instituciones utilizan el Border Gateway Protocol, o BGP, del protocolo de enrutamiento de "gateway" exterior para propagar información de enrutamiento. La gran mayoría de las empresas e instituciones con redes IP no necesitan un número de AS porque se encuentran bajo el control de una entidad más grande, como un ISP. Estas empresas utilizan protocolos de "gateway" interior como RIP, IGRP, EIGRP, OSPF o IS-IS, para realizar el enrutamiento de paquetes dentro de sus propias redes. Son una de muchas redes independientes dentro del sistema autónomo de ISP el cual es responsable del enrutamiento de paquetes dentro del sistema autónomo y entre otros sistemas autónomos.(Cisco Systems, 2006)

Características de BGP

BGP es un protocolo extremadamente complejo utilizado a través de Internet y dentro de empresas multinacionales, su función no es encontrar una red específica, sino proporcionar información que permita encontrar su AS en el cual se encuentra dicha red, las siguientes características demuestran por qué este protocolo es el mejor para routing exterior:

- Es un protocolo de routing path vector.
- BGP soporta VLSM, CIDR y sumarización.
- En el inicio de la sesión de envían actualizaciones completas; las actualizaciones por disparo se enviarán posteriormente.
- Se crean y mantienen las conexiones entre peers utilizando el puerto 179/TCP.
- La conexión se mantiene por keepalives periódicos.
- Cualquier cambio en la red resulta una actualización por disparo.
- Las métricas utilizadas por BGP, llamadas atributos, permiten gran granularidad en la selección del camino.
- El uso de direccionamiento jerárquico y la capacidad de manipular el flujo de tráfico son unas de las características que permiten al diseño de la red crecer.

- BGP tiene su propia tabla de routing, sin embargo, es capaz de compartir y preguntar sobre la tabla de routing IP interior.
- Es posible manipular el flujo de tráfico utilizando atributos. Esto significa que una ruta no puede enviar tráfico si el siguiente salto no quiere.
- Un de las mayores características distintivas de BGP son sus actualizaciones.
- A BGP no le interesa comunicar un conocimiento de cada subred de la organización, sólo le interesa utilizar suficiente información para encontrar un AS.
- Las actualizaciones de routing de BGP lleva la sumarización al extremo comunicando únicamente los números de los AS, prefijos de direcciones agregadas e información de routing basada en políticas.
- BGP asegura la fiabilidad del transporte llevando sus actualizaciones de routing y sincronizando las actualizaciones de routing. (Cisco Systems, 2016a) (Larios, A., Moreira, B., 2011)

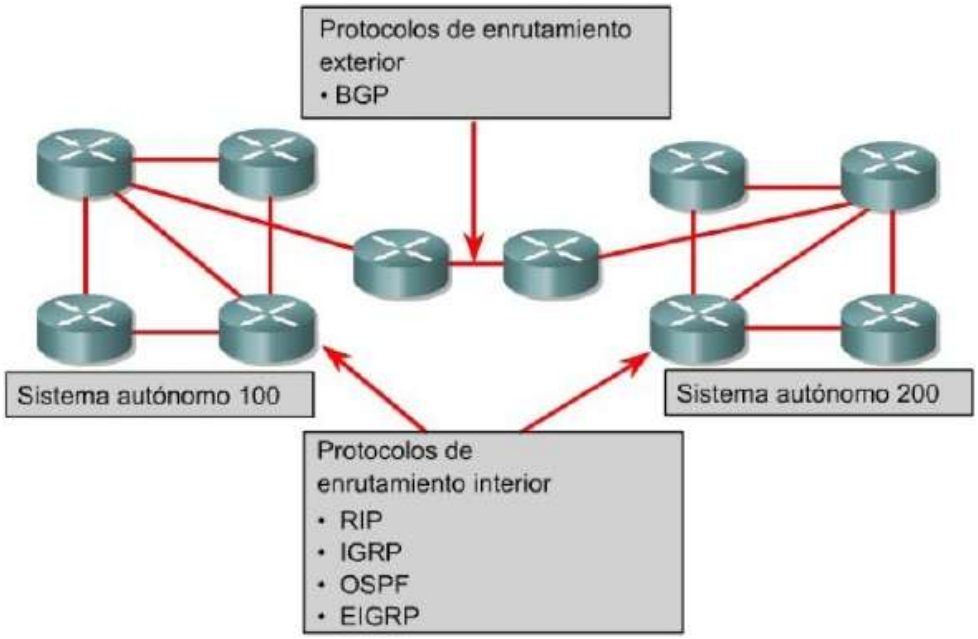


Figura 3-2: Protocolo de enrutamiento BGP
Fuente: (Larios, A., Moreira, B., 2011)

Tabla 3-2: Protocolos de enrutamiento avanzado

Protocolo	Interior/Exterior	Jerarquía Requerida	Métrica
OSPF	Estado del enlace	Sí	Coste
EIGRP	VD Avanzado	No	Compuesta
BGP	Vector de distancia	No	Path vectors o atributos

IS-IS	Interior	Sí	Coste

Realizado por: Fabián Hurtado, 2016
Fuente: *(Cisco Systems, 2016b)*

BGP puede ser implementado de diferentes formas:

- Entre AS: En este momento actúa como un protocolo de pasarela exterior, entonces lo llamaremos eBGP.
- Dentro de una AS: BGP se puede utilizar para llevar información exterior entre routers eBGP que residen en el mismo AS, entonces lo llamaremos iBGP.

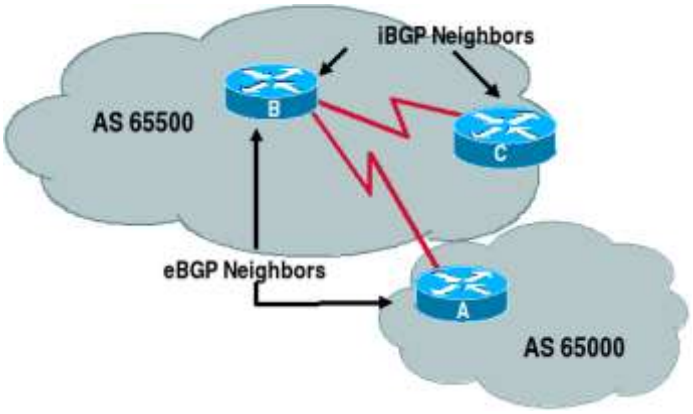


Figura 4-2: BGP interno y BGP externo

Fuente: (Cisco Systems, 2016a)

Características de Routers de Borde/Frontera ISP y Carrier

Tabla 4-2: Routers de Frontera más utilizados en ISP's Ecuatorianos – Características.

	Cisco ASR 9922	**Juniper MX2020**	**Huawei NE5000E**
Capacidad del Sistema	hasta 11 Tbps	hasta 80 Tbps	hasta 6,4 Tbps
Cantidad de Slots	20	20	16
Capacidad/Throughput de Slots	550 Gb/s	2Tbps	400 Gb/s
Procesador	2,27 Ghz Quad Core	1,8 Ghz Quad Core	1,5 Ghz Quad Core
Memoria base	8Gb base hasta 128 Gb modular	16Gb, 32Gb y 128Gb de base	16Gb/blade
Volumen de Storage	hasta 12 Gb	hasta 16 Gb	hasta 16 Gb
Sistema Operativo	Cisco IOS - XR	JunOS	VPR
Dimensiones	191x45x73	200x44x92	124x44x80
Matrix	Tarjeta dedicada	Tarjeta dedicada	Tarjeta dedicada
Soporte para interfaces ópticas 40Ge, 100G2	Sí	Sí	Sí
Peso en Kgs.	471	680	300

Soporte MPLS - BGP - IPv4 - IPv6	Sí	Sí	Sí
Administración de Red	SNMPv1, SNMPv2c, and SNMPv3.	SNMPv1, SNMPv2c, and SNMPv3.	SNMPv1 y SNMPv2c
Seguridad, Protección contra ataques, DDoS, IP Spoofing, etc.	Solo Detección DDoS	no	no
Temperatura de Operación	32 to 104°F (0 to 40°C)	32° to 104° F (0° to 40° C)	–40°C and +65°C

Realizado por: Fabián Hurtado, 2016
Fuente: (Cisco Systems, 2016c), (Juniper.com, 2015), (Huawei, 2015)

AS tiene la responsabilidad de informar a otros sistemas autónomos sobre cuáles son las redes que pueden alcanzar a través de ese AS y cada uno se identifica con un único número de AS (ASN), los que se controlan y se registran en internet, el ejemplo más común de AS es el ISP.

EL AS se aplica a todos los dispositivos de red dentro del dominio de enrutamiento del AS.

2.2 Monitoreo de Red

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de datos son actividades de gran relevancia para brindar un servicio de calidad a nuestros usuarios. De esto se deriva la importancia de un sistema capaz de notificar las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección del tráfico. Las redes de datos de las organizaciones, cada vez se vuelven mucho más complejas y la exigencia de operación es cada vez más demandante.

En la actualidad las redes, cada vez más soportan aplicaciones y servicios estratégicos de las organizaciones y si presentan algún tipo de desperfecto en su rendimiento, sin saber cuál es el punto de ruptura, puede causar pérdidas para la entidad u organización.
Por lo cual el análisis y monitoreo de red se ha convertido en una labor de mucha importancia y de carácter proactivo para evitar problemas a futuro.

La seguridad no solo radica en la prevención, sino también en la identificación. Entre menos tiempo haya pasado desde la intrusión e identificación, el daño será menor, para lograr esto es importante realizar un constante monitoreo del sistema con la finalidad de identificar vulnerabilidades en la red que los intrusos o el propio personal de la empresa puede hacer uso

para acceder a recursos de la red que no están autorizados y puedan causar denegaciones de servicio u otros problemas.

La prestación de servicios de calidad a los usuarios de una red depende en gran medida de factores que involucran aspectos de eficiencia y de seguridad. En el aspecto de eficiencia el ancho de banda disponible y la utilización que se haga del mismo representa un factor crítico, mientras en el caso de la seguridad, es importante conocer el tipo de tráfico que está siendo cursado por la red, así como tener la capacidad de detectar el tráfico malicioso.

2.2.1 Definición de Monitoreo

"Es el proceso de observar el comportamiento de la red y de sus nodos a través de la correspondiente información de administración. Esto se realiza con el fin de detectar fallas en la red y en los nodos. La Monitorización involucra dos factores importantes el tiempo de duración del monitoreo y el uso de recursos de la red. Mientras mayor sea el tiempo de monitoreo más efectiva será la detección de problemas, pero habrá una mayor ocupación de los recursos lo cual perjudicara a otras tareas. Por lo tanto debe existir un balance para conseguir un desempeño aceptable del sistema." (UNAM MX, 2005)

2.2.2 Enfoques del Monitoreo

Existen, dos formas de abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.

2.2.2.a Monitoreo Activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta, Este enfoque tiene la particularidad de agregar tráfico a la red. Es utilizado para medir el rendimiento de la red.

Técnicas de Monitoreo activo

Basado en ICMP

- Diagnosticar Problemas en la red.
- Detectar retardo, pérdida de paquetes.
- Disponibilidad de host de host y redes.

Basado en TCP

- Tasa de transferencia
- Diagnosticar problemas a nivel de aplicación.

Basado en UDP

- Pérdidas de paquete en un sentido (one-way)

2.2.2.b Monitoreo Pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico circundante por la red, se emplean diversos dispositivos como sniffers, ruteadores, computadores con software de análisis de tráfico y en general dispositivos con soporte snmp, rmon y netflow. Este enfoque no agrega tráfico a la red.

Técnicas de Monitoreo pasivo

Mediante SNMP

Utilizado para obtener estadísticas sobre la utilización de ancho de banda, consumo de recursos de red, etc., al mismo tiempo genera traps que indica que un evento inusual ha ocurrido.

Captura de tráfico

Se puede llevar a cabo de dos formas: 1) Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura. 2) Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura esta técnica es utilizada para contabilizar el tráfico que circula por la red.

Análisis de Tráfico

Usado para identificar el tipo de aplicaciones. Se puede implementar a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino etc. (UNAM MX, 2005)

2.3. HONEYPOTS

Según el Ing. Luis Alberto Pazmiño en su trabajo (Pazmiño, L., 2011) "honeypot es un sistema informático voluntariamente vulnerable a uno o más amenazas conocidas, destinadas a atraer a los atacantes informáticos para explorar sus estrategias de ataque", por lo que para esta investigación va a servir de vital ayuda ya que se va a simular un Router de Frontera que tenga vulnerable el puerto SNMP.

2.3.1. Tipos de Honeypots.

Se clasifican en 2 grupos:

Por su Interacción.

Por su implementación.

2.3.1.a. Por su Interacción

- **Honeypots de baja interaccion:** Básicamente son aquellos que simulan servicios como, por lo que no cuentan con un riesgo real, como FTP. Los más nombrados y utilizados son Tiny Honeypot, Valhala y Honeytrap

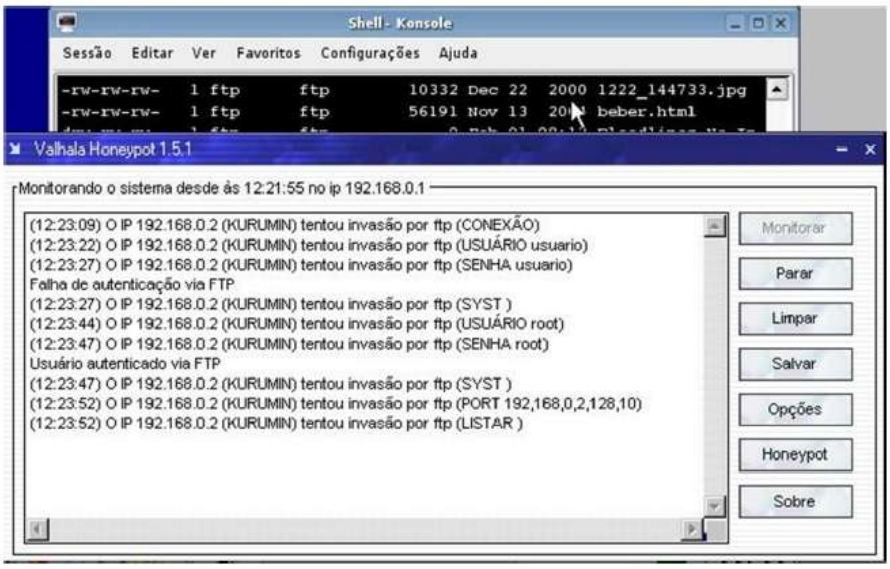


Figura 5-2: Honeypots de baja interacción
Fuente:*(Pazmiño, L., 2011)*

- **Honeypots de alta interacción:** Aumentan su riesgo para el uso ya que a diferencia del anterior, aquí se instalan y configuran servicios reales, instalados en una plataforma con S.O. y hardware no simulados. Este tipo de Honeypots envuelven al atacante en un entorno real de actividad, ya que el equipo puede formar parte de la red y de sistemas en producción. Aquí podremos recabar mayor información que con el anterior ya que el servicio cuenta con la complejidad ya acostumbrada y real.

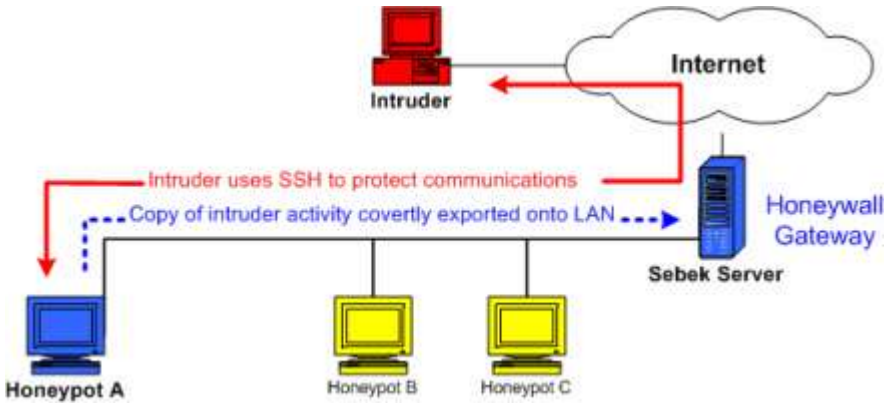


Figura 6-2: Honeypots de alta interacción
Fuente: (Pazmiño, L., 2011)

2.3.1.b Por su Implementación

- **Honeypots físicos:** Es instalado en una maquina física real por lo que se transforma en un Honeypot de alta interacción el cual correrá con los propios riesgos, a más del alto costo de mantenimiento y lo tedioso de la instalación.

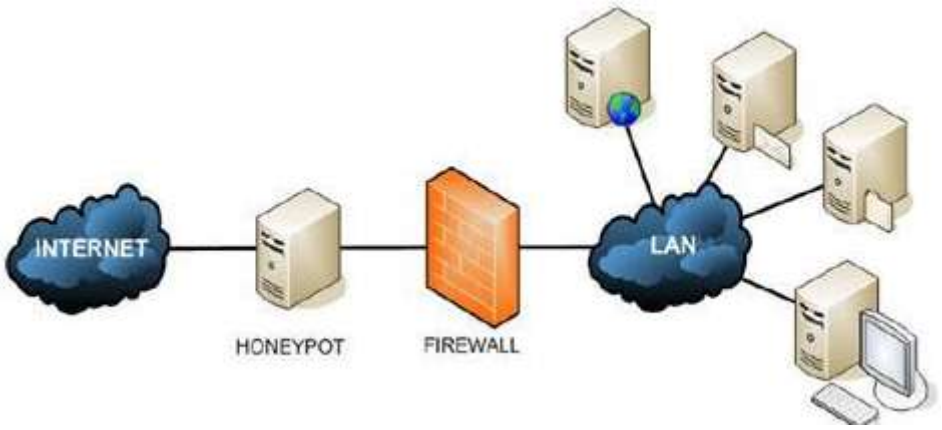


Figura 7-2: Honeypots físicos
Fuente: (Pazmiño, L., 2011)

- **Honeypots virtuales:** A diferencia del anterior, nacen con la ventaja de tener un gran espacio de direcciones IP ya que por espacio, movilidad y costo es difícil tener un Honeypot por cada dirección ip. En el Host físico se aprovecha la ventaja que al instalar varias máquinas virtuales se puede instalar la misma cantidad de Honeypot y asignarle una dirección Ip diferente.

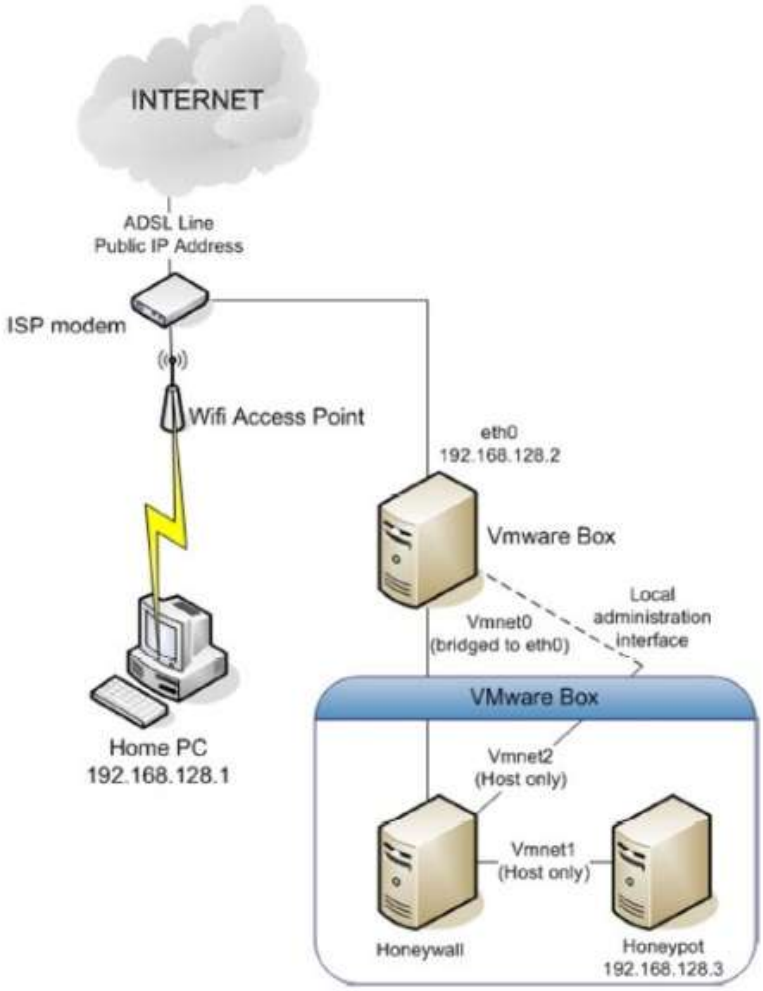


Figura 8-2: Honeypots virtuales
Fuente: (Pazmiño, L., 2011)

2.4 Recomendaciones de seguridad en Routers de Fronera

La ejecución de políticas y estándares para la seguridad de la información demanda la normalización y definición de recomendaciones para determinar, implementar y mejorar la seguridad, es por ello, que a nivel internacional se establecen parámetros específicos para la iniciación, implementación y mantenimiento de la seguridad de una organización, considerando que no todos las recomendaciones son aplicables para todas las situaciones, sin embargo, conllevan obligaciones legales para su cumplimiento. En este contexto, el presente trabajo de investigación considera las diferentes recomendaciones, normas y estándares de seguridad de la información aplicables en ambientes de redes WAN específicamente a Routers de Frontera. A continuación, se describen ciertas recomendaciones de seguridad obtenidas de estándares, metodologías y buenas prácticas, que han sido estudiadas y evaluadas por expertos a lo largo de los años.

2.4.1. Recomendaciones de seguridad de ISO/IEC 27001

Las normas ISO/IEC 27000, son un conjunto de estándares desarrollados (o en fase de desarrollo), por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.
La norma ISO/IEC 27001 "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Fecha de la de la versión española 29 noviembre de 2007. Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los SGSIs deberán ser certificados por auditores externos a las organizaciones. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002 (anteriormente denominada ISO 17799) (Honan, B., 2010).

Entre las recomendaciones finales enfocadas a comunicaciones WAN están:

1. Controlar los accesos a servicios internos y externos conectados en red..
2. Monitorizar constantemente el consumo de ancho de banda entre BR's.
3. Proteger la Disponibilidad de servicio de los BR.
4. Usar controles de seguridad o Firewalls.
5. Implementar herramientas de seguridad de red como IDS/IPS, gestión de vulnerabilidades, etc.

2.4.2 Recomendaciones de seguridad NIST

El NIST (National Institute of Standards and Technology) tiene como misión promover la innovación y la competitividad industrial mediante el avance ciencia de la medición, normas, y la tecnología de forma que mejoren la seguridad económica. En su publicación especial 800-82 (NIST National Institute of Standar and Technology, 2015) propone una recomendación especial para la seguridad de servicios de redes WAN:

"Desarrollar una arquitectura de seguridad para servicios de Administración de Redes WAN apropiada, tomando en cuenta que la protección y autenticación están dictados por los principios de la seguridad que son: Confidencialidad, Integridad, Disponibilidad, los mismos que al ser quebrantados generan vulnerabilidades (a los que se asocia un ataque)"

2.4.3 Recomendaciones de seguridad CISCO

La empresa multinacional Cisco Systems Inc. (Cisco Systems, 2016b) líder desde hace casi 30 años en tecnologías WAN según el Cuadrante Magico de Gartner, da las siguientes recomendaciones:

1. Asegurar todos los elementos de la red como servidores, protocolos, dispositivos finales y prioridades entre otros.
2. Aplicar firewalls, IDS, IPS y SBCs para analizar el tráfico.
3. Deshabilitar puertos que no se están usando en los switches corporativos y reforzar las políticas de seguridad.
4. Apagar todos los servicios innecesarios o aplicaciones ejecutándose en servidores, firewalls, routers de acceso y otros dispositivos de la red.
5. Emplear direccionamiento IP estático en la red y no utilizar IP dinámicas.

CAPITULO III

3. METODOLOGIA DE INVESTIGACION

3.1 Diseño de la investigación

La presente investigación se enmarca dentro de un estudio **Cuasi-Experimental** en los cuales los sujetos o grupos de estudio no están asignados aleatoriamente, es decir, los contenidos a ser enviados en el ambiente de pruebas no serán al azar, sino que se los tendrá definidos antes de realizar dicho ambiente por el investigador.

Además, se manipula una variable independiente y evaluación de su correspondiente efecto en la variable dependiente. Su validez se alcanza a medida que se demuestre que los ataques perpetrados hacia el protocolo SNMP de un HONEYPOT – ROUTER puedan ser Detectados y Prevenidos a tiempo, escogiendo la tecnología adecuada en función de las contramedidas frente al análisis realizado a los registros guardados y generados.

3.2 Tipo de investigación

En la investigación se considera que el tipo de estudio que se va a realizar es una **investigación descriptiva y aplicada**, ya que se utilizara el conocimiento para realizar un estudio comparativo de los ataques informáticos realizados hacia el protocolo SNMP frente a las herramientas diseñadas para monitorear, detectar, analizar y prevenir dichos ataques.

3.2.1. Métodos de Investigación

En este punto, se describe los métodos teóricos-prácticos que se maneja en la investigación, los cuales ayudan a obtener información teórica y deducir la misma:

Método Científico: Mediante este método en la investigación se pudo buscar información en libros, revistas, artículos científicos e Internet, lo que da lugar a detectar los problemas

fundamentales, para lograr esta investigación, porque a través de estos se transmite las posibles soluciones del caso.

Método Analítico: Este método se aplica durante la etapa de análisis donde se recopilo la información necesaria, para tener una idea clara, de lo que se va a realizar durante a investigación, para tener una idea clara, de lo que se va a realizar durante la investigación, es decir, se puntualizará que es lo que se debe hacer y cómo hacerlo, para determinar las vulnerabilidades en el protocolo SNMP y los ataques a los que están expuestos los Routers de Frontera.

Experimental: Este método consiste en provocar voluntariamente una situación que se requiere estudiar, para modificar o alterar, es decir que se diseñan ambientes de simulación, para realizar las pruebas necesarias, y analizar los resultados obtenidos de modo que permitan determinar los mecanismos de defensa apropiados.

3.2.2. Técnicas

Se usarán ciertas técnicas, entre ellas están:

- Observación.
- Recopilación de información.
- Análisis.
- Pruebas

3.2.3 Fuentes de información

Revisión de información de fuentes bibliografías como:

- Textos
- Revistas
- Documentos
- RFC’s
- Otros

3.2.4. Recursos

a) Recursos humanos

Dentro la parte humana intervienen:

- Ejecutor de tesis

- El Tutor
- Los Miembros
- Proveedores de Equipos

b) Recursos materiales

- Hojas Papel Bond
- CD’s
- Flash Memory
- Bibliografía
- Internet (meses)

c) Recursos técnicos

Tabla 1-3: Recursos Técnicos

RECURSO	CARACTERISTICA	DESCRIPCION
Computador de Escritorio	Procesador Intel core I5 2.5 ghz; Memoria Ram 12; Disco Duro 40GB; Tarjeta Fastethernet	Computador dedicado a ser la vez de Atacante
Router CISCO	Modelo 7206 - IOS c7200nm-adventerprisek9-mz.12-4.T1.bin	Router ISP-AS / Frontera
Computador de Escritorio	Procesador Intel Pentium IV 2.2 Ghz; Memoria Ram 512 Mb; Disco Duro 20GB; 3 Tarjetas Fastethernet 1 Gbps.	Computador configurado como Firewall
Switch Cisco	Modelo 2960 IOS c2960-lanbasek9-mz.122-25.fx.bin	Switch correspondiente a la Red LAN
Switch Cisco	Modelo 2960 IOS c2960-lanbasek9-mz.122-25.fx.bin	Switch correspondiente a la DMZ
Router CISCO	Modelo 7206 - IOS c7200nm-adventerprisek9-mz.12-4.T1.bin	Router Honeypot
Laptop 1	Procesador Intel core I5 2.5 ghz; Memoria Ram 12; Disco Duro 40GB; Tarjeta Fastethernet 10/100 Mbps	1 - Prueba de Prevención y Detección de Intrusos
Laptop 2	Procesador Intel core I5 2.5 ghz; Memoria Ram 12; Disco Duro 40GB; Tarjeta Fastethernet 10/100 Mbps	2 - Prueba de Prevención y Detección de Intrusos
Linux Centos 6.7	Versión MINIMAL 64 bits centos-6.7-x86_64-minimal.iso	Sistema Operativo utilizado como base de instalación del Firewall
Wireshark	Versión 2.0.1 para Linux Ubuntu x86	Analizador de Protocolos de Red

Kali Linux 2.0 / 64bits	Versión 2.0 64 bits kali-linux-2.0-amd64.iso	Software de pruebas de penetración
Ubuntu 14.04 / 64bits	Linux Ubuntu versión Desktop 14.04 para 64 bits ubuntu-14.04.4-desktop-amd64.iso	Sistema Operativo utilizado como base de instalación del Software IDPS 1 e IDPS 2
SNORT	IDPS para Ubuntu 14.04 Versión 2.9, MySQL, Apache2, ACIDBASE	Sistema de Detención y Prevención de Intruciones – 1
TShark	Versión 2.0.0 para Centos (no usar 1.7.9)	Analizador de protocolos – texto
VMWare Workstation	Versión 11.0 para procesadores 64bits	Software de Virtualización de Sistemas Operativos
GNS3	Versión 1.3.3 GLP v3 - 64bits	Simulador gráfico de Routers Cisco

Realizado por: Fabián Hurtado, 2016

3.3 Planteamiento de la hipótesis

Con el análisis de los resultados de una honeypot virtual, se conseguirá mitigar los riesgos generados por la intrusión en routers de frontera, incrementando su disponibilidad y confiabilidad.

3.3.1 Determinación de las variables

La variable dependiente esta designada por lo siguiente: Mecanismos para mitigar riesgos generados por la intrusión en routers de frontera.

La variable independiente esta designada por lo siguiente: Resultados producto del análisis en una Honeypot virtual.

3.4 Operacionalización conceptual de variables

Tabla 2-3: Operacionalización de Variables

VARIABLES	TIPO	CONCEPTO
Mecanismos para mitigar riesgos generados por la intrusión en routers de frontera.	Variable Dependiente	Es el conjunto de medidas que se pueden tomar para contrarrestar o minimizar los impactos. El propósito de la mitigación es la reducción de la vulnerabilidad.

Resultados producto del análisis en una Honeypot virtual.	Variable Independiente	Estudio de los ataques y vulnerabilidades atraídos por un Honeypot Router y dirigidos al protocolo SNMP de un Router.

Realizado por: Fabián Hurtado, 2016

3.5 Operacionalización metodológica de variables

Tabla 3-3: Operacionalización metodológica de variables

VARIABLES	TIPO	INDICADORES	INDICES	TECNICA
Mitigará los riesgos generados por la intrusión en routers de frontera.	Variable Dependiente	Ingreso del ataque	control de acceso	Observación, Análisis
		Detección de ataques	configuración de scripts para detección de ataques	Observación, Análisis
		Prevención de ataques	configuración de scripts para prevención de ataques	Observación, Análisis
El análisis de los resultados de una Honeypot virtual.	Variable Independiente	Afectación del Performance físico por sus Vulnerabilidades	Utilización de la CPU y Memoria	Software de prueba
		Determinar las amenazas.	Ataques, tipos de ataques, clasificación según su efecto	Recopilación de información
		Determinar el impacto producido por los ataques	Clasificación de Amenazas por su impacto.	Análisis
		Riesgo	Estimación de Amenazas y Vulnerabilidades	Fórmulas

Realizado por: Fabián Hurtado, 2016

3.6 Población y muestra

3.6.1 Población

Según reportes de seguridad de la compañía Cisco Systems, señalan que desde el año 1997 hasta la actualidad se continúan realizando estudios sobre vulnerabilidades que generan riesgos de seguridad en varios de sus protocolos de enrutamiento como RIP, OSOF, EIGRP y BGP (protocolo utilizado en Routers de Frontera), donde el rastreo de puertos se evidencio como su amenaza más recurrente. Cisco asegura que desde el 2014 se registra un alto crecimiento de en

ataques al impedimento de la continuidad y denegación de servicio, accediendo por un protocolo muy poco tomado en cuenta en su seguridad, SNMP.

Figura 1-3: Informe Cisco sobre amenazas
Fuente: (Cisco Systems, 2016d)
Realizado por: Fabián Hurtado, 2016

En vista que la seguridad a los protocolos de enrutamiento (RIP, OSOF, EIGRP y BGP) de Routers de Frontera son los que cuenta con mayor cantidad de investigaciones, el presente trabajo se centra en el estudio de Vulnerabilidades y Riesgos con las que cuenta el Protocolo Simple de Administración de Red SNMP, el mismo, que representa la población a estudiar.

3.6.2 Muestra

Para la selección de la muestra se deberá realizar un análisis de las Amenazas y Vulnerabilidades con los que cuenta el protocolo simple de administración de red SNMP.

3.6.2.a Amenazas y Vulnerabilidades

Casi todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy.

La seguridad de la información es más que un problema de seguridad de datos en los computadores; debe estar básicamente orientada a proteger la propiedad intelectual y la información importante de las organizaciones y de las personas.

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones.

Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.

3.6.2.b TIPOS DE AMENAZAS

Actualmente, existen 3 amenazas que no han sido cubiertas, aunque, en 1998 se creó la versión 3 del protocolo, por lo cual, atacantes informáticos se siguen aprovechando de sus vulnerabilidades para realizar ataques con éxito.

Se presenta la siguiente tabla de amenazas de acuerdo al análisis realizado por la Ing. Ruth Crespata Almachi en su tesis (Crespata, R., 2012)

Tabla 4-3: Amenazas en protocolo SNMP

AMENAZA	SNMP V1	SNMP V2	SNMP V3
DENEGACION DE SERVICIO	No proporciona seguridad	No proporciona seguridad	No proporciona seguridad. Ya que cualquier entidad puede causar una Denegación de Servicio a través de herramientas que generen tráfico y desborden los dispositivos intermedios o finales.
ANALISIS DE TRAFICO / RASTREO DE PUERTOS	No proporciona seguridad	No proporciona seguridad	No proporciona seguridad. A causa de que los desarrolladores de la versión consideraron que en dicho momento no era necesario.

ATAQUE DE FUERZA BRUTA	No proporciona seguridad	No proporciona seguridad	No proporciona seguridad. Todas las versiones de SNMP están sujetos a la fuerza bruta y ataques de diccionario para adivinar las cadenas de comunidad, cadenas de autenticación, las claves de autenticación, cadenas de cifrado o claves de cifrado, ya que no implementan un protocolo de enlace de desafío-respuesta. (Crespata, R., 2012)
SUPLANTACIÓN DE IDENTIDAD	No proporciona seguridad	No proporciona seguridad	Utiliza la autenticación para validar los mensajes SNMP
MODIFICACIÓN DEL FLUJO DE MENSAJES	No proporciona seguridad	No proporciona seguridad	Hace uso de marcas de tiempo para asegurarse que los mensajes vienen de entidades autorizadas, haciendo que se cumpla la ventana temporal
GESTIÓN DE RED CENTRALIZADA	Permite	Permite	Permite
GESTION DE RED DISTRIBUIDA	No permite, no facilita la comunicación entre gestores	Introduce PDU informRequest que permite el intercambio de información de gestión entre gestores, dando paso a la Gestión de red distribuida y principalmente permitiendo la descongestión de equipos	Hereda las mismas operaciones de SNMPv2 por lo tanto permite una gestión distribuida, permitiendo a si la existencia de dos o más estaciones que hagan de máquinas gestoras, dependiendo de la complejidad de la red
GESTION DE RED JERARQUICA	No permite, por la misma razón que no se admite la gestión de red jerárquica	Como permite la administración de red distribuida también admite la gestión jerárquica	Hereda las mismas operaciones de SNMPv2 por lo tanto permite una gestión jerárquica

Realizado por: Fabián Hurtado, 2016
Fuente: (Crespata, R., 2012)

3.6.2.c Vulnerabilidades / Debilidades del protocolo SNMP

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene.

La seguridad en los protocolos de protección y autenticación están dictados por los principios de la seguridad que son: Confidencialidad, Integridad, Disponibilidad, los mismos que al ser quebrantados generan vulnerabilidades (a los que se asocia un ataque) los que son apropiados y convenientes para los fines de esta investigación. Esta población se seleccionó basándose en los documentos de la NIST (National Institute of Standards and Technology)(NIST National Institute of Standar and Technology, 2007) (NIST National Institute of Standar and Technology, 2015)

Tabla 5-3: Impacto de vulnerabilidades SNMP

PRINCIPIO DE SEG. AFECTADO	VULNERABILIDAD / DEBILIDAD	IMPACTO
DISPONIBILIDAD	1- Comunicación basada en UDP (no orientada a la conexión) y por motivos de eficiencia, los datos se envían y se reciben sin verificar la conexión con el origen o destino de la misma y se da por hecho la correcta entrega o recepción de datos. 2- SNMP permite que se realicen consultas de gran volumen a través del tipo de solicitud llamado "GetBulkRequest", esta solicitud en la V2c y V3 se caracteriza por que el tamaño de su respuesta (423-1560 Bytes) es mucho más grande que el de la solicitud (0-102 Bytes).	1- La comunicación basada en UDP al no verificar la conexión de Origen/Destino y dar por hecho la correcta entrega o recepción de datos, nos permite modificar/suplantar la dirección IP origen dando pie al "IP spoofing". 2- Las consultas GetBulkRequest crean un efecto de amplificación, ya que la respuesta siempre será más grande que la solicitud. El servidor SNMP responderá con respuestas de gran tamaño y esto multiplicado por la cantidad de peticiones, producirá un aumento en el volumen de información neto que fluye a través el sistema, lo cual va íntimamente ligado con la velocidad real de transferencia de datos en la red, medida en Mbit/s o también llamado THROUGHPUT, el cual siempre tiene que ser menor al ancho de banda. Elevan la utilización de la CPU y Memoria con mucha facilidad y velocidad. (Security By Default, 2014)

CONFIDENCIALIDAD Y DISPONIBILIDAD	SNMP permite la realizar rastreos de puertos y análisis de tráfico, contramedida no desarrollada desde su creación.	Según la consulta realizada hacia un equipo determinado, se puede obtener y el estado de cualquier puerto.
CONFIDENCIALIDAD	Cadenas de autenticaciones expuestas y accesibles.	Al obtener el atacante la cadena de autenticación (comunidad), se puede hacer pasar como elemento Manager uniéndose a la misma comunidad para monitorizar, acceder, cambiar la configuración del equipo monitorizado.

Realizado por: Fabián Hurtado, 2016

Se ha determinado la utilización de una muestra no aleatoria, tomando del cuadro de amenazas las mismas que no proporcionan seguridad en las 3 versiones del protocolo y que muchos de ellos hacen ataques basándose en los resultados de otros o son los mismos ataques con pequeños cambios.

Las amenazas a ser evaluadas son las siguientes:

Tabla 6-3: Amenazas a evaluar

AMENAZA
DENEGACION DE SERVICIO
ANALISIS DE TRAFICO / RASTREO DE PUERTOS
ATAQUE DE FUERZA BRUTA

Realizado por: Fabián Hurtado, 2016

3.7 Instrumentos de recolección de datos

Luego de haber reconocido a profundidad las amenazas y vulnerabilidades del protocolo SNMP, se medirán las contramedidas frente a los ataques asociados a dichas vulnerabilidades, mediante herramientas de Auditoria Informática. De acuerdo a los procedimientos generales establecidos se ha determinado la utilización del siguiente software con herramientas de Pentesting, Análisis / Rastreo, Detección y Ruptura.

Tabla 7-3: Herramientas para ejecución de ataques

TIPO DE USO	HERRAMIENTA
Ataque de denegación de servicios distribuido	Kali Linux - "snmp-DDOS", Tshark
Scanners, y Rastreador de puertos	Kali Linux – NMAP, Tshark, Wireshark
Ataque de fuerza bruta	Kali Linux - "snmp-brute"

Realizado por: Fabián Hurtado, 2016

Tomando en cuenta que para la Detección y Prevención de amenazas existen varias herramientas tanto comerciales como basadas en Software Libre, se realizó una selección exhaustiva, ya que la tecnología a elegir tenía cumplir con diversos parámetros y características dependiendo de factores tanto humanos, económicos y de infraestructura, aquí citados:

1. El perfil de los administradores, sus conocimientos en determinados sistemas operativos.
2. Recursos económicos disponibles.
3. El instrumental de red con el que se cuenta.

Para la asignación de pesos o valores de la tabla se consideró la escala de Likert que significa 1: Totalmente insatisfactorio 2: Insatisfactorio 3: Medianamente satisfactorio 4: Satisfactorio 5: Totalmente satisfactorio (Ray Poynter, 2012)

Tabla 8-3: Análisis comparativo entre las Soluciones IDS/IPS Software Libre

CARACTERISTICAS	SECURITY ONION	SNORT	SURICATA
Modo mixto ids/ips	3	5	5
Ataque fuerza bruta/DDOS/Rastreo	5	5	5
Soporta MIB - getBulk	5	5	5
Modo sniffing	5	5	5
Network Brifge mode - Inline	1	5	5
Interfaz gráfica para administración	5	5	1
Estadísticas	5	5	1
Actualizaciones sin costo	1	5	5
facilidad de implementación	5	5	1
Soporte y documentación	1	5	5
Calificación	36	50	33

Realizado por: Fabián Hurtado, 2016

Por medio de este resultado obtenido mediante pruebas de laboratorio, nos damos cuenta que la herramienta SNORT cumple ampliamente con los parámetros y características de infraestructura, humano y económico, por lo cual es la seleccionada.

3.8 Propuestas de Solución

Todo proceso de investigación, requiere el apoyo de metodologías, trabajos y literatura especializada que guíen y respalden los procesos que se llevan a cabo, razón por la cual, se detallan las metodologías idóneas para esta investigación, por ser las más acordes y que cubren los puntos necesarios para dar cumplimiento a los objetivos de la presente investigación.

En este punto se analiza el paper indexado en la revista científica del "Institute of Electrical and Electronics Engineers – IEEE" como es el Paper: Honeypot Router for routing protocols protection (Ghourabi, A., Abbes, T., Bouhoula, A., 2010), el libro publicado por la editorial Addison-Wesley llamado Honeypots, tracking hackers (Spitzner, L, 2016), y la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información PAe - MAGERIT v.3 expedita de acuerdo al Decreto Real de Marzo/2010, por medio del cual se regula el Esquema Nacional de Seguridad Española.(Portal de Administración Electrónica, 2014)

El Paper indexado en la revista científica del "Institute of Electrical and Electronics Engineers – IEEE" llamado Honeypot Router for routing protocols protection (Ghourabi, A., Abbes, T., Bouhoula, A., 2010), habla de la experiencia de los investigadores al momento de realizar la planificación de atracción, lectura de Logs (registros) y los cálculos técnicos al momento de realizar todos los estudios de las vulnerabilidades, como cada una generaba riesgos con alza en el porcentaje al impacto de los protocolos de enrutamiento más comunes como, Rip, OSPF, EIGRP y BGP; este documento indica el cómo, cuándo y porque utilizar un Honeypot basado en un Sistema Operativo de Routers marca Cisco. Ayuda bastante al investigador con la filosofía "FIRST STUDIED AND THEN ACTED" traducido al español sería "Primero estúdielo y luego actúe" haciendo una analogía que un médico primero estudia la VULNERABILIDAD de su paciente y luego le da la receta exacta para CURARLO.

El libro publicado por la editorial Addison-Wesley llamado Honeypots, tracking hackers (Spitzner, L, 2016) El libro ayuda a construir y desplegar soluciones propias Honeypot en el lugar exacto de su infraestructura de red y cada uno de los pasos a seguir para que los atacantes no sepan que están siendo filtrados; también da las pautas de cómo realizar un verdadero análisis de vulnerabilidades entiempo real y que herramientas utilizar de manera general. Aquí se revisan métodos de penetración que utilizan los atacantes de todo nivel tales como:

Evaluación de Riesgos
Auditoria de Seguridad
Hacking Ético
Búsqueda de Vulnerabilidades
Escaneo de Seguridades
Test de Intrusión

Según el autor realiza un estudio de 1.000.000 de ataques en el lapso de 30, donde se tabula entrada tras entrada y resultado de las amenazas visualizadas, detectadas y prevenidas. Estos ataques analizados alcanzan porcentajes muy altos de riesgo, incrementando problemas en los principios de seguridad Disponibilidad y Confidencialidad, tales como:

Análisis de Puertos
Obtención de Datos
Denegación de Servicio

Para la medición y valoración matemática de todo lo que se genera dentro de los Routers de Frontera, se utilizó la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información PAe - MAGERIT v.3 (Portal de Administración Electrónica, 2014) expedita de acuerdo al Decreto Real de Marzo/2010, por medio del cual se regula el Esquema Nacional de Seguridad Española. Esta metodología es la más utilizada desde su creación ya que la Certificación ISO/IEC 27001, inclusive, la recomienda por sus famosas tablas de coeficiente y fórmulas creadas y diseñadas a través de los años para la medición real de la Amenaza, Vulnerabilidad, Riesgo e Impacto, ítems necesarios con los cuales se elaboran gráficos estadísticos para comparación de resultados.

Luego de estos estudios previos podemos y fusionando sus conceptos, recomendaciones y experiencias de sus creadores, podemos definir la solución llamada: HONEYPOT ROUTER SNMP, el cual consta de 2 componentes, los cuales conseguirán mitigar los riesgos generados por la intrusión en Routers de Frontera basados en los resultados de un Honeypot Virtual:

Infraestructura de Solución: La cual contiene 2 etapas a) Estudio y detección de vulnerabilidades y ataques, b) Aplicar la protección y medidas de seguridad
Mecanismos de Prevención: Los cuales son un complemento de la Infraestructura anterior, con lo cual se completan los pasos para la detección y prevención de amenazas.

3.9 Ambiente de Simulación y pruebas

Para el ambiente de pruebas de esta investigación, se tuvo que contar con la aprobación del director de la academia CISCO en el mes de Diciembre de 2015, ya que fue necesario la investigación sobre los equipos que se encontraban en el Laboratorio Cisco de la ESPOCH

3.9.1 Ambiente de pruebas 1: Infraestructura de Solución Vulnerable

Para el siguiente ambiente de pruebas simulando la INFRAESTRUCTURA DE SOLUCIÓN VULNERABLE, se utilizó el software de virtualización de Routers Cisco GNS3 ver. 1.3.3 combinado con el software de virtualización de sistemas operativos VMWare Workstation ver. 11.0.

Esta simulación describe un ambiente de tecnología utilizado en la mayoría de empresas ISP donde se destacan 3 Zonas WAN (Wan del Atacante, ISP2 e ISP2) cada una identificada con su número identificador de Sistema Autónomo, la única diferencia con la infraestructura tradicional es que se tiene instalado un Honeypot y un IDS (SNORT) que estará analizando y recopilando una serie de ataques que sufra el Router de Frontera escondido, el cual posee una configuración técnica normal del protocolo SNMP v2c, interfaces, ruteo, etc., con el fin de que cuando se realicen los ataques, el pirata informático no note que es una especie de señuelo, por medio del cual él será estudiado.

Este ambiente simulado, sugiere que, el firewall, al ser un dispositivo de capa 4 que lee por puertos, publique el protocolo SNMP hacia los otros AS Sistemas Autónomos, con el fin de comunicar las consolas NMS con dispositivos administrados. Luego de realizar el ataque, cualquiera que este fuere, el Router Honeypot, enviará una copia del tráfico hacia el equipo con el IDS SNORT instalado con el fin de analizar todos los paquetes. El atacante efectúa escaneo y rastreo de puertos, ataques de denegación de servicio y ataque de diccionario o fuerza bruta, los cuales fueron realizados con éxito.

Muy a pesar de tener reconocimiento de toda amenaza que existente en la red hacia los Routers de Borde, no deja de ser un ambiente totalmente vulnerable.

INFRAESTRUCTURA DE SOLUCIÓN VULNERABLE

ETAPA 1

Estudio y detección de vulnerabilidades y ataques

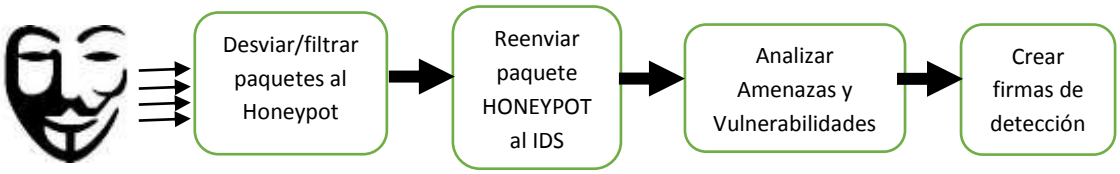


Figura 2-3: Esquema de Solución 1ra. Etapa
Realizado por: Fabián Hurtado, 2016

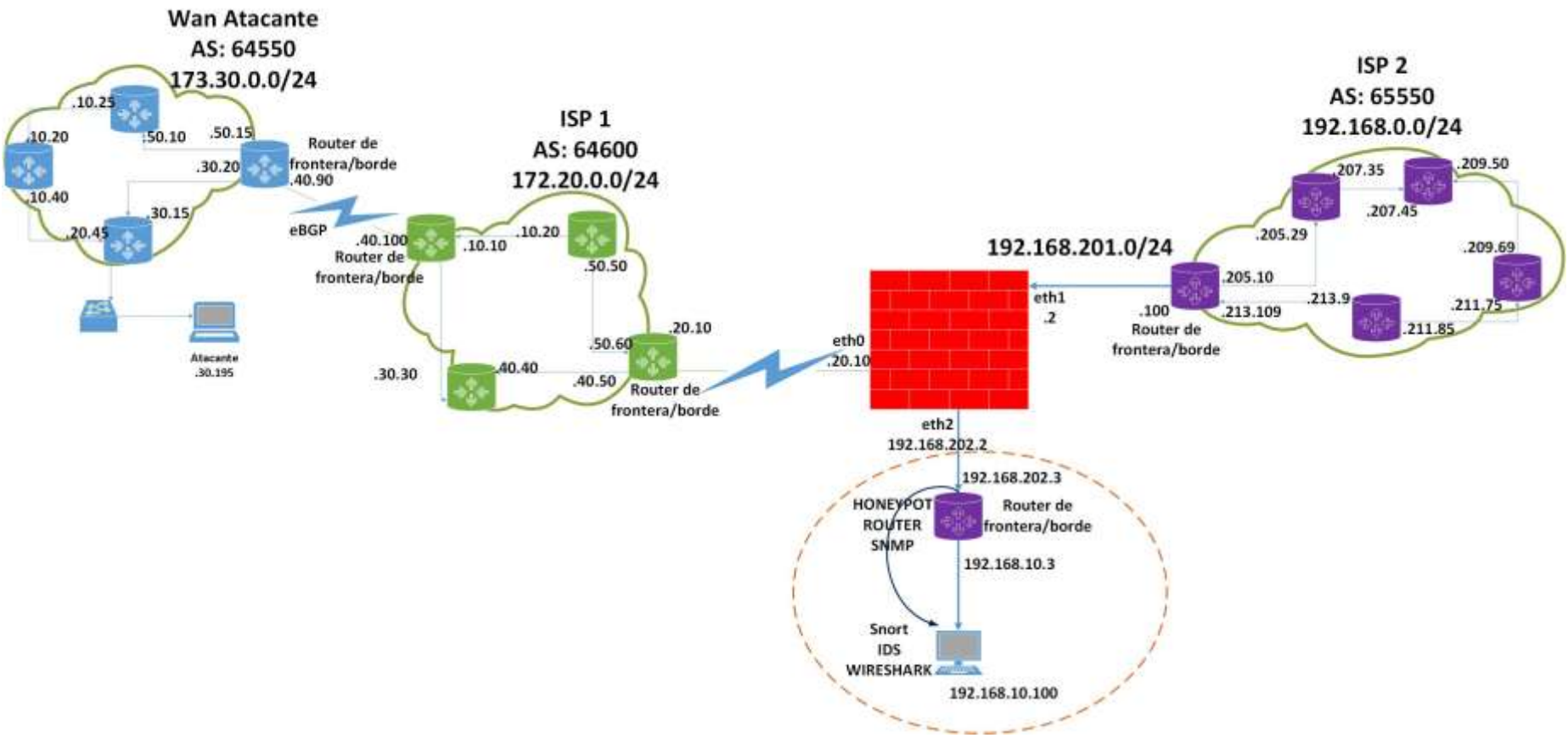


Figura 3-3: Infraestructura de Solución Vulnerable
Realizado por: Fabián Hurtado, 2016

3.9.2 Ambiente de pruebas 2: Infraestructura de Solución Protegida

Descripción:

Para el siguiente ambiente de pruebas simulando la INFRAESTRUCTURA DE SOLUCIÓN PROTEGIDA, se volvió a contar con el software de virtualización de Routers Cisco GNS3 ver. 1.3.3 combinado con el software de virtualización de sistemas operativos VMWare Workstation ver. 11.0.

Esta simulación describe la solución propuesta donde se sugiere la instalación de un sistema NIDS/NIPS – Sistema de Detección / Prevención de Intrusos basado en RED (monitorean la red en busca de tráfico de red sospechoso al analizar la actividad por protocolo de comunicación) con 2 interfaces de red en modo Bridge "br0" entre el Firewall y el AS-Sistema Autónomo que se dese proteger de ataques, en este caso en particular, protegerá al Router de Borde del ISP2 simulado en con una infraestructura robusta de Honeypot-Router de todos los ataques que el Firewall no sea capaz de detectar e ingresen por la interfaz eth2.

El atacante efectúa nuevamente escaneo, rastreo de puertos, ataques de denegación de servicio y ataque de diccionario o fuerza bruta, los cuales NO fueron realizados con éxito ya que el sistema NIDS lo detecta y el NIPS los bloquea, dejando sin efecto dichos ataques y dando una segunda capa de seguridad a la red.

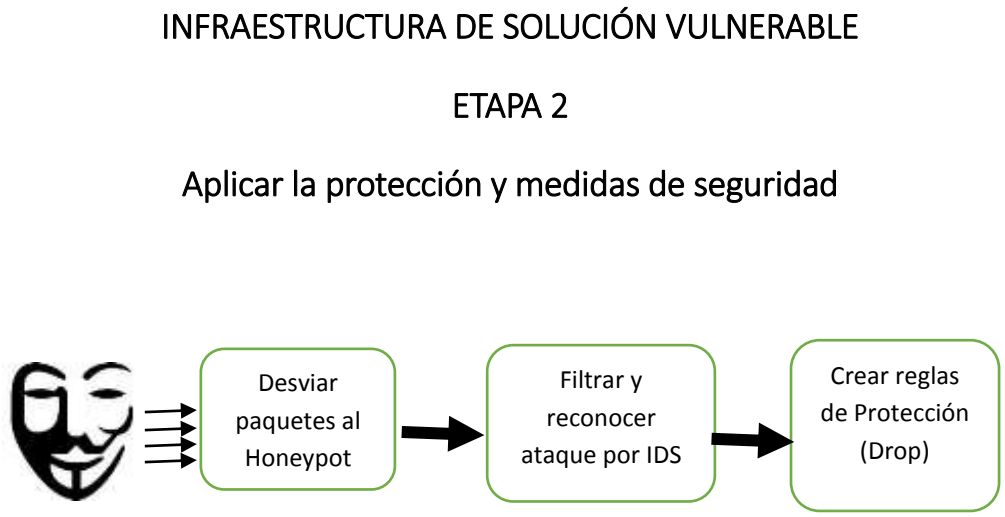


Figura 4-3: Esquema de Solución 2da. Etapa
Realizado por: Fabián Hurtado, 2016

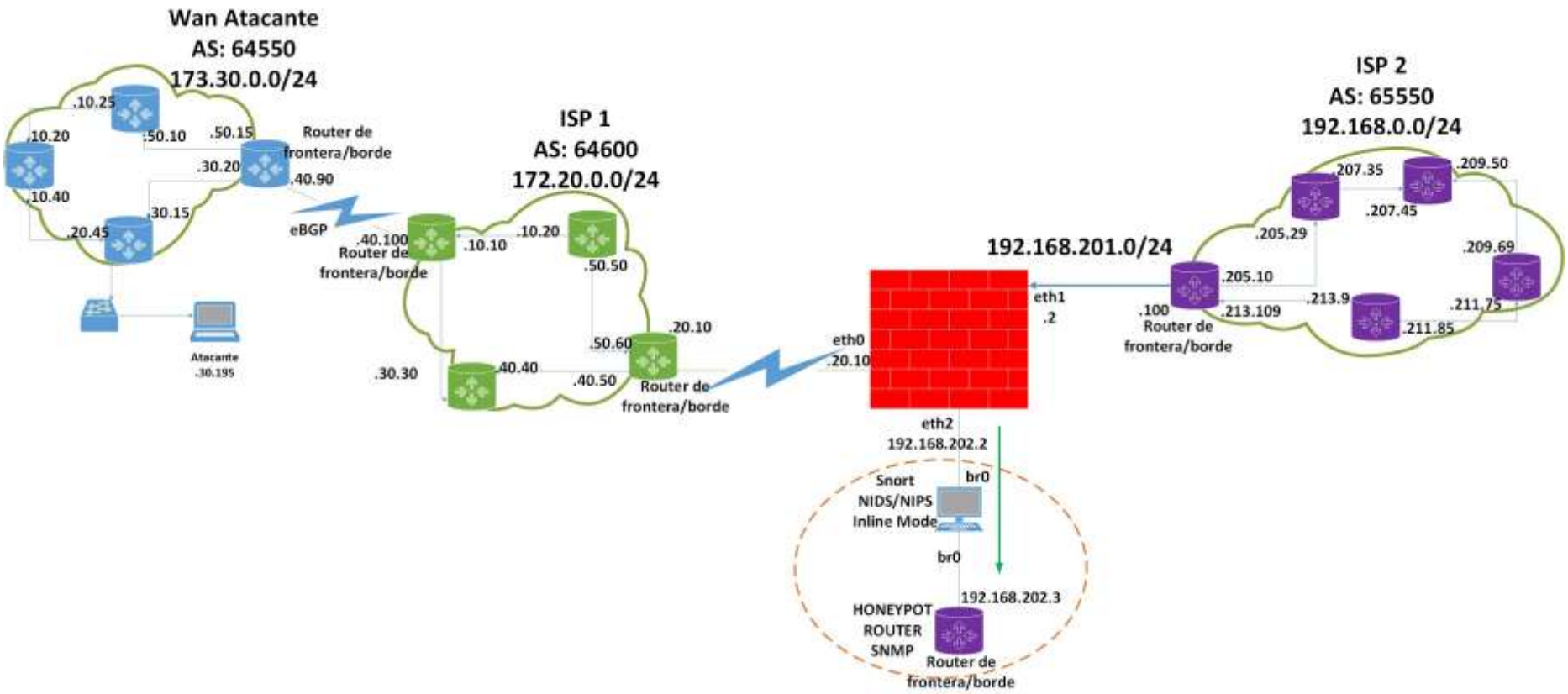


Figura 5-3: Infraestructura de Solución Protegida
Realizado por: Fabián Hurtado, 2016

CAPITULO IV

4. RESULTADOS Y DISCUSIÓN

4.1. Identificación de los Activos Relevantes

Basados en el interés del atacante y bajo los puertos protegidos en el ambiente seguro, estos no podrán continuar llevándose a cabo, o no podrán concebirse por muchos intentos que estos realicen.

El atacante efectúa nuevamente escaneo y rastreo de puertos, ataques de denegación de servicio y ataque de diccionario o fuerza bruta, los cuales NO fueron realizados con éxito ya que el sistema NIDS lo detecta y el NIPS los bloquea, dejando sin efecto dichos ataques y dando una segunda capa de seguridad a la red. Tomando en cuenta estos parámetros de seguridad se generan los resultados de la siguiente manera:

Dentro de los aspectos de control y seguridad la amenaza que mantenía el Router al permitir a los atacantes entrar de forma fácil a identificar los procesos del sistema, bajo la vulnerabilidad del propio dispositivo, conllevo a que la visualización se mantuviera en un 33%, la posibilidad de plagiar información del sitio o de la base de datos de los computadores del área de estudio en un 66% y la facilidad para inhabilitar el Servidor en un 99%, datos referidos al 100%.

En este punto el impacto generado es bastante alto del cual la información corporativa corre el riesgo de pérdidas y generación de múltiples falencias que perjudicarían al escenario de estudio donde se realizó el análisis. De acuerdo con la metodología MAGERIT v3.0, se muestra la siguiente tabla que soporta la medición del impacto generado a enrutadores: (Portal de Administración Electrónica, 2014)

Tabla 1-4. Escala de Impacto MAGERIT v3.0

IMPACTO	
Bajo	0% - 25%
Intermedio	26% - 50%
Alto	51% - 75%
Muy Alto	> 76%

Fuente: (Portal de Administración Electrónica, 2014)
Realizado por: Fabián Hurtado, 2016

Dentro de los parámetros de Seguridad el Router que se encontraba vulnerable, se generaron los siguientes resultados, tomando en cuenta la fórmula para el cálculo de Vulnerabilidad Informática sugerida en la metodología MAGERIT v 3.0 (Portal de Administración Electrónica, 2014)

Vulnerabilidad = performance proc. + performance mem.

En este punto y siguiendo la formula antes indicada se puede evidenciar que el grado de vulnerabilidad es alto comparado con otros factores de riesgo.

Tabla 2-4. Performance tomado del Router Atacado – ambiente vulnerable

ATAQUES	UTILZ. CPU	UTILZ. MEM.	VULNERABILIDAD	
DDOS 0,99 3PC's	75,00%	80,00%	155,00%	4
F.Bruta 0,66	18,00%	16,50%	34,50%	2
Rastreo Ptos. 0,33	1,00%	5,20%	6,20%	1

Realizado por: Fabián Hurtado, 2016

Figura 1-4. Impacto antes de intervención
Realizado por: Fabián Hurtado, 2016

Dentro de los parámetros de seguridad, este tipo de investigación generó resultados de los cuales se pudo comprobar que los riesgos superaban el intervalo normal. Para su cálculo el cual

este es muy alto, se utilizó la fórmula y escala sugerida también por la metodología MAGERIT v3.0 (Portal de Administración Electrónica, 2014)

Tabla 3-4. Escala de Amenazas Informáticas MAGERIT v3.0

AMENAZA	
View Information	0,33
Information Gathering	0,66
Disable Services	0,99

Fuente: (Portal de Administración Electrónica, 2014)
Realizado por: Fabián Hurtado, 2016

Luego de utilizar la fórmula del riesgo, obtenemos los siguientes resultados:

Riesgo = Amenazas x Vulnerabilidad

Tabla 4-4. Análisis de Riesgo

AMENAZA	VULNERABILIDAD	IMPACTO	RIESGO
DDOS	155,00%	Muy Alto	153%
F.Bruta	34,50%	Intermedio	23%
Rastreo Ptos.	6,20%	Bajo	2%

Realizado por: Fabián Hurtado, 2016

Figura 2-4: Análisis de Riesgo
Realizado por: Fabián Hurtado, 2016

De la comparación que se realizó entre el antes y después se desprende una notable disminución en el riesgo ante los ataques generados.

Acorde al Impacto generado, resulta muy alto el 155,00% en el DDOS, intermedio el 23% F. Bruta y el 2% bajo en rastreo de puertos.

El resultado matemático, conlleva a verificar el nivel o grado de vulnerabilidad que tendrá el Router de Frontera, tomando en cuenta las mismas formulas y escalas sugeridas por la metodología MAGERIT v 3.0, el cual da como resultado lo siguiente:

Tabla 5-4: Calculo de Vulnerabilidad después de Solución

ATAQUES	UTILZ. CPU	UTILZ. MEM.	VULNERABILIDAD
DDoS x 3 PC's	3,00%	18,09%	21,09%
F.Bruta	5,00%	8,98%	13,98%
Rastreo Puertos	1,00%	5,23%	6,23%

Realizado por: Fabián Hurtado, 2016

Como se puede observar, los valores disminuyeron considerablemente luego de configurar la solución, generando un 21.09% en DDOS en comparación al antes (155%), 13,98% en Fuerza Bruta comparados con el antes (34,50%) y se mantienen el Rastreo de Puertos con un 6,23%

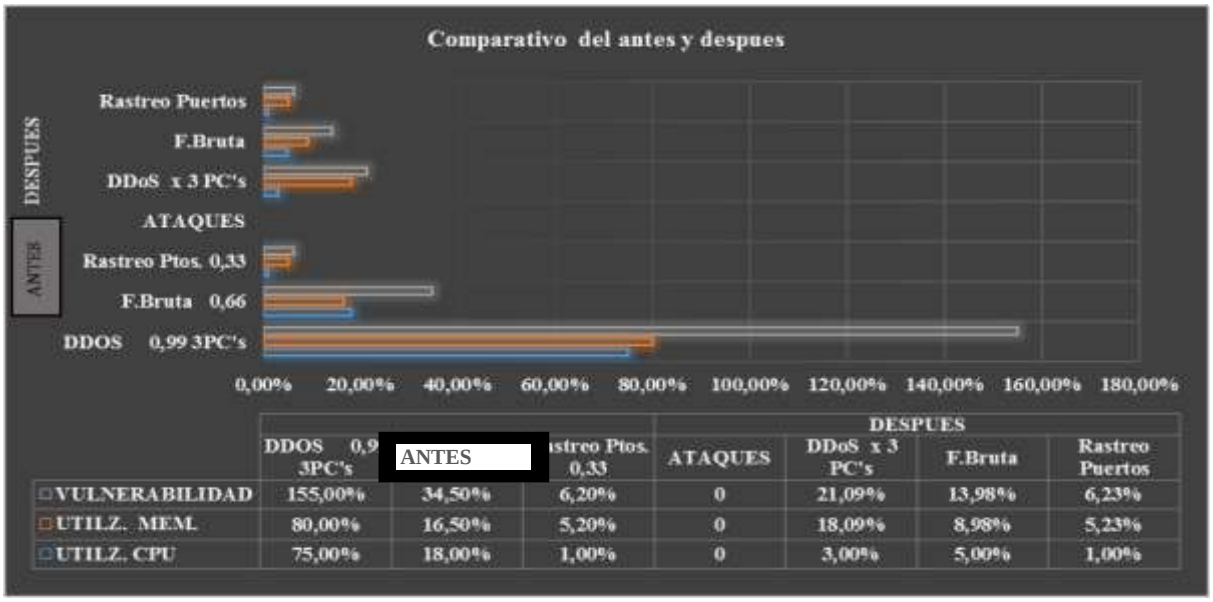


Figura 3-4: Vulnerabilidad antes y después
Realizado por: Fabián Hurtado, 2016

En cuanto al riesgo, se tornó controlado luego de la intervención y aplicación de seguridad en el Router de frontera, para esto DDOS que antes generaba un 153%, después de la intervención se encuentra en el 21,09%, F. Bruta antes era de 23% y luego de la intervención esta se tornó en 9%, el referente de Rastreos de Puertos, se mantuvo ya que después de la intervención se generó en el 2,00%.

Tabla 6-4: Cálculo de Riesgo después de la solución

AMENAZA	VULNERABILIDAD	IMPACTO	RIESGO
DDOS	21,09%	Bajo	21%
F.Bruta	13,98%	Bajo	9%
Rastreo Ptos.	6,23%	Bajo	2%

Realizado por: Fabián Hurtado, 2016

Figura 4-4: Riesgo después de la solución
Realizado por: Fabián Hurtado, 2016

Como se puede identificar en el comparativo, antes de generar el tipo de protección o barrera para los atacantes, el riesgo era bastante alto del cual en la actualidad pudo ser disminuido considerablemente una vez aplicada la barrera/bloqueo, generando como punto principal que si funciona el tipo de solución que se pretende lograr.

Figura 5-4. Amenazas antes y después

Realizado por: Fabián Hurtado, 2016

Dentro del Gráfico, se indica claramente como las amenazas antes de la intervención generaban problemas ante la seguridad en la entrada al Router de Frontera, en el cual, el riesgo era muy alto generando en el DDOS 155% el mismo que se pudo disminuir en más del 89% a igual que los demás puntos que han reducido considerablemente su situación a través de la barrera expuesta.

Se puede comprobar que la situación actual bajo los resultados planteados, han generado la oportunidad de protección, los mismos que brindan una situación de confianza ante futuros ataques.

4.2. Resultados

Dentro de los resultados, el objetivo es disminuir el riesgo en el Router de Frontera, para lo cual se clasificó por categoría la escala cualitativa: 1, 2, 3, 4 o B, I, A, Ma, tal como lo recomienda la metodología MAGERIT (Portal de Administración Electrónica, 2014). Se pudo identificar en esta escala el impacto señalado anteriormente, acorde a la siguiente tabla.

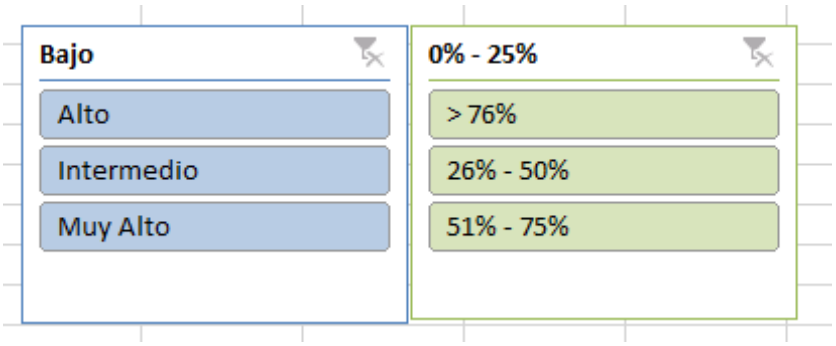


Figura 6-4: Escala de Impacto

Fuente: (Portal de Administración Electrónica, 2014)

4.2.1. Validación de Variables

Se pretendió lograr validar las variables dependientes e independientes, tomando los resultados de investigación bajo los ensayos ya identificados en el desarrollo, para lograr este tipo de validación, se consideró verificar lo siguiente:

Variable Dependiente

Mitigar los riesgos generados por la intrusión en Routers de frontera.

Tabla 7-4: Variable Dependiente

Indicadores	VALOR
Ingreso del ataque control de acceso (con freeware: Wireshark y Tshark)	3,63
Detección de ataques Se detectan ataques con Scripts	5,00
Prevención de ataques Se previenen ataques con scripts	4,5

Realizado por: Fabián Hurtado, 2016

Variable Independiente: Análisis de los resultados de Una Honeypot virtual

Tabla 8-4: Variable Independiente

Indicadores

Vulnerabilidades		**MEM**	**CPU**
Utilización de la CPU	**DDOS**	4	4
y Memoria	**F.Bruta**	2	2
	Rastreo Ptos.	1	1

Determinar Amenazas		**Nivel de Afectación**
Ataques, tipos de	**DDOS**	4
ataque, clasificación	**F.Bruta**	2
según su efecto	**Rastreo Ptos.**	1

Determinar el Impacto		**Impacto**
Clasificación de Ame-	**DDOS**	Ma
nazas por su impacto	**F.Bruta**	I
	Rastreo Ptos.	B

Riesgo		**Riesgo**
Estimación de	**DDOS**	4
Amenazas y Vulnerabi-	**F.Bruta**	2
Lidades	**Rastreo Ptos.**	1

Realizado por: Fabián Hurtado, 2016

4.2.2. Validación matemática de la Hipótesis

Ho = Los controles basados en Honeypot Router han generado bloqueos ante ataques previstos y verificados, esto permitirá proteger la información interna del AS-Sistema Autónomo, ya que no hará vulnerable al router de frontera.

H_a: En base a la aplicación del Honeypot Router, es favorable en su aplicación al sistema de protección desde el Router $P \leq 0.75$

Nivel de Significación:

$\ddot{\alpha} = 0.05$

Criterio:

½

Rechazo de la H_o Si $P\ x \geq 18 / \sum_{x=18}^{25}$

$\sum_{x=18}^{25}$ = Chi cuadrado calculado

$\sum_{x=½}^{3,87}$ = Chi cuadrado de tabla

Tabla 9-4: Tabla de contingencia de lo observado

Indicadores	**VALOR**
Ingreso del ataque control de acceso (con freeware: Wireshark y Tshark)	3,63
Detección de ataques Se detectan ataques con scripts	5,00
Prevención de ataques Se previenen ataques con scripts	4,6

Realizado por: Fabián Hurtado, 2016

Los valores correspondientes a los indicadores de la Tabla 9-4, fueron calculados gracias a la Escala de comportamiento tipo Likert, detallada en el Anexo A2 y la Tabla 10-4, la cual se encuentra también detallada en el Anexo A1.

La siguiente formula presenta el cálculo esperado bajo el tipo de frecuencia generada

p= 0,0492

$$F_e = \frac{(total\_fila)(total\_columna)}{\mu}$$

En base a los resultados esperados y lo observado acorde al Chi cuadrado ($\sum_{x=18}^{25}$) con la siguiente formula:

$$\hat{\alpha} = \sum_{x=18}^{25} \begin{bmatrix} 25 \\ x \end{bmatrix} (1/2)^8 (1/2)^{25-x}$$

Donde:

25x = el número observado de ataques

($½^8$) = Calculo ante seguridad del Honeypot, integrado a un porcentaje de protección alto > 76

$(½)^{25=X}$= es la sumatoria del porcentaje bajo por resultados esperados.

Tabla 10-4: Tabla de cálculo del Chi Cuadrado

		$\sum_{x=18}^{25}$	**(25x) ½⁸**	**(½)25$^{=x}$**	**El análisis, detección y prevención de las vulnerabilidades basadas en el Honeypot-Router, pretendió mitigar los riesgos generados por la intrusión en Routers de frontera.**
# Pruebas		**Ingreso de ataque**	**Detección de ataque**	**Prevención de ataque**	**Observaciones**
prueba 1	día1	1	5	1	No visualiza, detecta 3, no prev (config)
prueba 2	día2	1	5	1	No visualiza, detecta 3, no prev (config)
prueba 3	día3	1	5	1	No visualiza, detecta 3, no prev (config)
prueba 4	día4	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 5	día5	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 6	día6	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 7	día7	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 8	día8	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 9	día9	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 10	día10	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 11	día11	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 12	día12	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 13	día13	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 14	día14	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 15	día15	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 16	día16	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 17	día17	5	5	5	ingresa, detecta, previene
prueba 18	día18	5	5	5	ingresa, detecta, previene
prueba 19	día19	5	5	5	ingresa, detecta, previene
prueba 20	día20	5	5	5	ingresa, detecta, previene

prueba 21	día21	5	5	5	ingresa, detecta, previene
prueba 22	día22	5	5	5	ingresa, detecta, previene
prueba 23	día23	5	5	5	ingresa, detecta, previene
prueba 24	día24	5	5	5	ingresa, detecta, previene
prueba 25	día25	5	5	5	ingresa, detecta, previene
prueba 26	día26	5	5	5	ingresa, detecta, previene
prueba 27	día27	5	5	5	ingresa, detecta, previene
prueba 28	día28	5	5	5	ingresa, detecta, previene
prueba 29	día29	5	5	5	ingresa, detecta, previene
prueba 30	día30	5	5	5	ingresa, detecta, previene
Total		119	150	138	
Likert		3,6333	5	4,6	

Realizado por: Fabián Hurtado, 2016

La explicación detallada de las Observaciones de la Tabla 10-4 como el cálculo de los Totales, se encuentran en el Anexo A1.

Se determina el grado de libertad que se obtiene del número de filas y el número de columnas de la Tabla de Contingencia.

Donde:

K= número de filas

J= número de columnas

V= (h-1)(j-1)= grados de libertad

En este caso

K= 4

J= 3

V = (4-1)(3-1)= 6 grado de libertad

El valor del Chi cuadrado $\sum_{x=18}^{25}$ se presenta en el desarrollo acorde al porcentaje de resultados favorables > 76 y se determina su explicación por procesos en el anexo A1.

Decisión:

Si la probabilidad es alta se considera que la información bajo la base de datos está en común acuerdo con el HONEYPOT como solución, lo cual indica que la aplicación de este sistema de seguridad no genera una solución completa para todo el sistema, ya que utiliza solo el Router para un solo punto específico y no para las redes complementarias en el sector o institución

donde se aplicó el estudio. En este punto al generar la probabilidad alta, se identifica que la aplicación del Honeypot Router sí establece un tipo de solución factible ante la seguridad de red a través de prevención/bloqueo que se propone como solución.

Probabilidad y nivel de confianza: ǎ = 0.05 = a 0.007 = 0,95

Grados de Libertad: n =6

Valor de Referencia del Chi Cuadrado $\sum_{x=18}^{25}$ = 12,592

Valor de Chi cuadrado encontrado $\sum_{x=½}^{3,87}$ = 15,595

$$\hat{\alpha} = P(x \geq 18 \mid p = ½)$$

$$\hat{\alpha} = \sum_{x=18}^{25} \left[\begin{matrix}25\\x\end{matrix}\right] (1/2)^{8} (1/2)^{25-x}$$

$$\hat{\alpha} = 0.007$$

Tabla 11-4: Cálculo de Frecuencias Obtenidas, (fo)

Estudio/ Resultado	Ingreso de ataque	Detección de ataque	Prevención de ataque	Total
Malo	3	15	3	21
Regular	12	20	20	52
Buenos	34	45	45	124
Excelente	70	70	70	210
Total	119	150	138	**407**

Realizado por: Fabián Hurtado, 2016

Nivel de Significancia= 0,05

Grados de libertad= (4filas-1) x (3col-1) = 6

$$\chi^2 = \sum \frac{(fo - ft)^2}{ft}$$

Frecuencia Teórica	X2
6,176	1,634
17,647	0,314
34,412	1,596
61,765	1,098
7,721	6,863
22,059	0,192

43,015	0,092
77,206	0,673
7,103	2,37
20,294	0,004
39,574	0,744
71,029	0,015
	15,6

Tabla 12-4. Tabla de cálculo de Frecuencia Teórica (ft) y Chi-Cuadrado
Realizado por: Fabián Hurtado, 2016

X2 tabla= 12,592 - X2 encontrado= 15,595

Degrees of Freedom	Possibility of Chance Occurrence in Percentage (5% or Less Considered Significant)								
	90%	80%	70%	50%	30%	20%	10%	5%	1%
1	0.016	0.064	0.148	0.455	1.074	1.642	2.706	3.841	6.635
2	0.211	0.446	0.713	1.386	2.408	3.219	4.605	5.991	9.210
3	0.584	1.005	1.424	2.366	3.665	4.642	6.251	7.815	11.341
4	1.064	1.649	2.195	3.357	4.878	5.989	7.779	9.488	13.277
5	1.610	2.343	3.000	4.351	6.064	7.289	9.236	11.070	15.086
6	2.204	3.070	3.828	5.348	7.231	8.558	10.645	12.592	16.812
7	2.833	3.822	4.671	6.346	8.383	9.083	12.017	14.067	18.475

Tabla 13-4: Tabla del 5% de Significancia
Realizado por: Fabián Hurtado, 2016

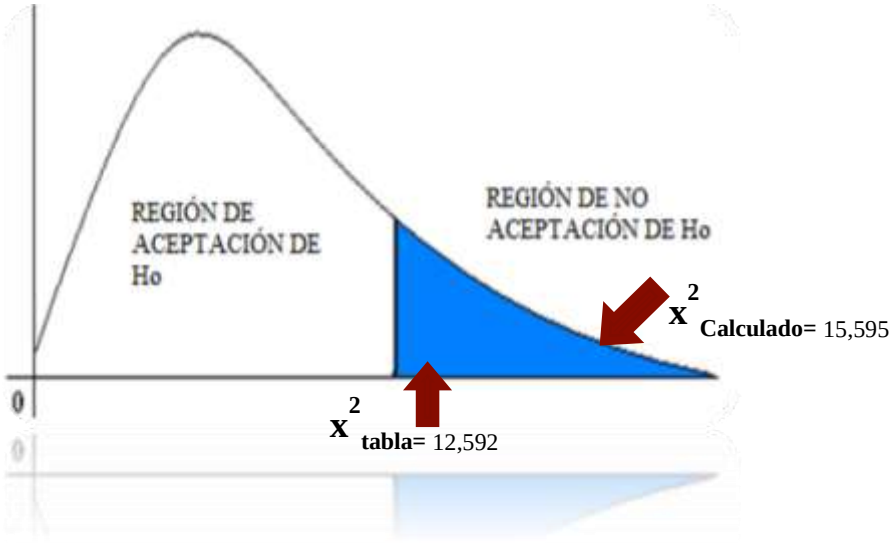


Figura 7-4: Gráfico para demostración
Realizado por: Fabián Hurtado, 2016

Con el empleo de la estadística inferencial chi-cuadrado y un nivel de significancia de 0.05, de acuerdo a la tabla de distribución se obtiene que X2 Tabla 12.592 y el valor calculado X2 Calculado en esta investigación es de 15.292, notando que es superior al valor de la tabla de distribución, por lo que el valor de X2calculado se encuentra en el sector de NO Aceptación de Ho y resulta estadísticamente significativa, Aceptando la hipótesis de investigación Hi.

CAPITULO V

5. PROPUESTA

5.1 Descripción

En el presente trabajo de investigación, cada una de las etapas fué realizada de forma muy ardua, aunque existieron muchos problemas. Hubieron más CONTRAS que PROs, ya que como autor y maestrante, la seguridad es un tema que me apasiona, pero el desconocimiento de que herramienta era la más idónea para trabajar, por la gran cantidad de software existente en el mercado, comercial y sin costo, llega a confundir bastante. Luego de instalar, probar en laboratorio, evaluar y conversar con sus equipos de desarrollo, se seleccionaron 6 herramientas, todas ellas excelentes en su campo de acción, las cuales son:

1. Syslog de Centos
2. Bro IPS
3. OSSIM Alien Vault
4. Security Onion
5. Snort
6. Suricata

De estas 6 herramientas, se decide que las más apropiadas por su funcionamiento, información resultante, y tener cubierto un alto porcentaje de los Riesgos de Seguridad producto de las vulnerabilidades y amenazas encontradas en el protocolo SNMP, eran las 3 últimas:

1. Security Onion
2. Snort
3. Suricata

De acuerdo a la metodología MAGERIT v3.0 (Portal de Administración Electrónica, 2014) , los Riesgos de Seguridades se resumen en los siguientes:

Riesgo Alto

El hecho de detener el correcto funcionamiento de un servicio o equipo (intermedio/final) hace de este riesgo de Nivel ALTO.

La comunicación basada en UDP no verifica la conexión de Origen/Destino y da por hecho la correcta entrega o recepción de datos, lo que da paso a un proceso llamado “IP SPOOFING” el cual permite modificar/suplantar la dirección IP origen al momento de que el pirata informático realice su ataque.

El proceso de consulta GetBulkRequest propio del protocolo, crea un efecto de amplificación, ya que, para efecto del ataque, la respuesta siempre será más grande que la solicitud. El servidor SNMP responderá con respuestas de gran tamaño y esto multiplicado por la cantidad de peticiones, producirá un aumento en el volumen de información neto que fluye a través del sistema. Esto traerá consecuencias directas con la velocidad real de transferencia de datos medida en Mbits/s, y al no soportarlo, el performance del equipo reproductor de requerimientos GetBulk literalmente colapsará, como por ejemplo ocurre en ataques como DDOS “Distributed Denial Of Service”, los cuales elevan el porcentaje de utilización de la CPU y Memoria con mucha facilidad y velocidad.

Riesgo Intermedio

El hecho de obtener información que sirva de parámetro complementario para realizar ataques y no detener el correcto funcionamiento de un servicio o equipo (intermedio/final) hace de este riesgo de Nivel INTERMEDIO.

Por lo investigado, las cadenas de autenticaciones son expuestas con un alto grado de accesibilidad, y aunque en un bajo porcentaje, podrían adivinarse las claves de autenticación, o claves de cifrado, si estas claves se generan a partir de contraseñas cortas (débiles), o contraseñas que se pueden encontrar en un diccionario muy bien elaborado, al obtener el atacante la cadena de autenticación (comunidad), este, se puede hacer pasar como elemento Manager uniéndose a la misma comunidad y este parámetro es clave para realizar formas de ataque más letales Ataque de Fuerza Bruta y de Diccionario.

Riesgo Bajo

El hecho de poder visualizar información que ayude a decidir que tipio de ataque se va a realizar, sin que sirva de parámetro complementario para realizar ataques y no detenga el correcto funcionamiento de un servicio o equipo (intermedio/final) hace de este riesgo de Nivel BAJO.

Según la consulta realizada hacia un equipo determinado, se puede obtener como resultado el estado de cualquier conjunto de reglas para comunicación. Hasta la actualidad los desarrolladores del protocolo no han creado o configurado una contramedida para esta amenaza ya que, desde su creación, consideraron que no era necesario.

5.2 Análisis y diseño de la solución propuesta

La tecnología propuesta como solución en esta investigación consiste en combinar las fortalezas del anticipo y la prevención ante lo que denominamos "intrusos" con la reducción de posibles vulnerabilidades en el equipo que supone la primera fase de seguridad de toda empresa, como es el FIREWALL, garantizando la Disponibilidad y Confiabilidad de los datos, 2 de los 3 principios de la Seguridad.

Este esquema se compone de 3 fases fundamentales:

1. Análisis de Amenazas

En esta primera fase se analizan todos los ataques recibido ya sea por medio del equipo Firewall (modo texto) o en la solución HONEYPOT-ROUTER.

Si el análisis es realizado en el Firewall, se lo efectúa por medio del capturador de paquetes Tshark (Open Souce) el cual es un Wireshark (freeware) en modo texto, tomando en cuenta que, por la naturaleza de la topología de red utilizada en la mayoría de empresas, el Firewall es la primera o la única barrera que brinda seguridad a la infraestructura interna, con esta herramienta, el análisis consiste en ir verificando en tiempo real los detalles de cada uno de los paquetes de lo que para nuestro juicio denominamos un "ingreso o petición no adecuada".

Contrario a esto, el otro análisis se lo realiza en la solución HONEYPOT-ROUTER, equipo "señuelo" diseñado para atrapar todos los ataques realizados a la infraestructura interna del AS. Dicho equipo contiene configuraciones típicas de un enrutador de frontera o borde, que atraerá a

los atacantes por medio de la configuración del protocolo SNMP v2c. La función principal de este equipo es enviar una copia del tráfico generado en una de sus interfaces entrantes hacia otro equipo, el cual, tiene instalado un IPS (Sistema de Detección de Intrusos), donde se almacena todo lo que ocurra en la interfaz del HONEYPOT-ROUTER.

La configuración para exportar el tráfico entrante por la interfaz FastEthernet 0/0 hacia la FastEthernet 0/1 es la siguiente.

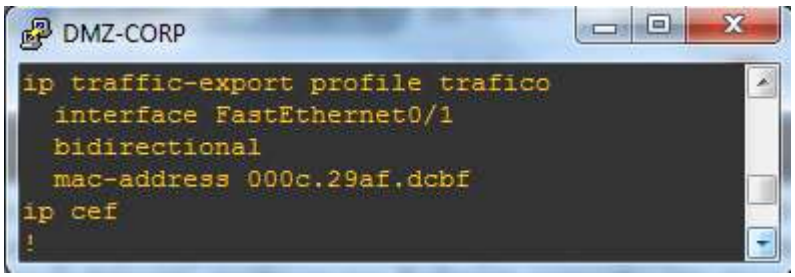


Figura 1-5: Configuración IP TRAFFIC
Realizado por: Fabián Hurtado, 2016

Luego activamos el perfil "trafico" en la interfaz FastEthernet 0/0 y listo.

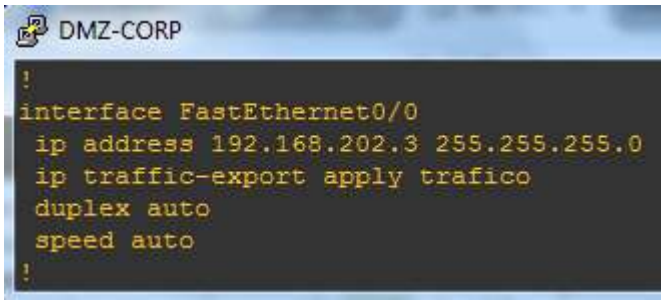


Figura 2-5: Activación IP TRAFFIC en Fe0/0
Realizado por: Fabián Hurtado, 2016

Una de las ventajas de este software IPS instalado en el otro externo del HONEYPOT-ROUTER, tal como se lo muestra en la Figura 3-5, es que genera un historial por tipo de protocolo y por periodos de tiempo, lo cual ayuda a que el análisis para la detección de todos los "ingresos o peticiones no adecuadas" sea exacto.

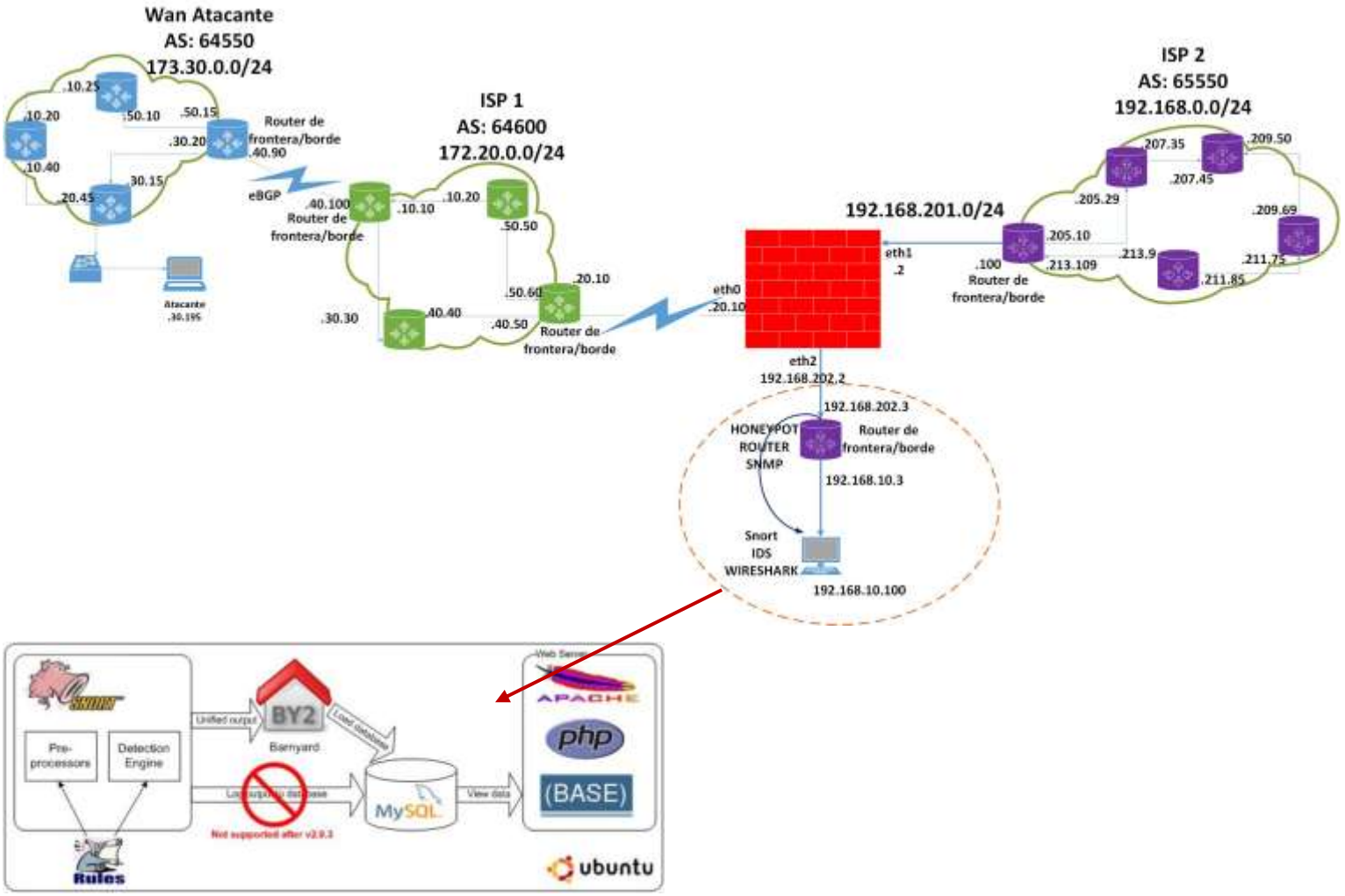


Figura 3-5: Infraestructura de Solución Vulnerable
Realizado por: Fabián Hurtado, 2016

Otra ventaja del IDS (Snort) es que, en su instalación se interconecta con el Spooler Barnyard2 el cual envía el resultado de lo detectado por el motor /sensor de Detección hacia una base de datos MySQL, así mismo, el visualizador web ACIDBASE lee la base de datos y visualiza los eventos de forma gráfica y mucho más detallada que Tshark, haciendo el trabajo más amigable al Oficial de Seguridad, encargado permanentemente de la revisión de los mismos.

2. Instalación NIDS/NIPS

En esta etapa y con la ayuda de un excelente manual (Instalador IDS/IPS Linuca, 2008), es donde se instala una variación del IPS (Sistema de Prevención de Intrusos, lugar donde se establecen políticas de seguridad para proteger al equipo o a la red de un ataque) llamada NIPS, el cual bloquea todos los ataques que circulan en la red, previo a la configuración de políticas resultantes del análisis realizado por un IDS/NIDS, analizador de red, Sniffer, etc.

Para el éxito de esta etapa, se debían cuidar muy bien los detalles, ya que al ser este, un proceso de producción, donde todos los ataques van a ser bloqueados, se debe tener mucho cuidado de que los parámetros de detección hayan sido exactos para los bloqueos funcionen y no permitan que se vea afectado el funcionamiento y performance de los equipos, adicionalmente hay que destacar que el sistema SNORT tiene los 2 sensores/motores, tanto de Detección como de Prevención, siendo esta una ventaja en costos, ya que al momento de detectar más amenazas no sería necesario comprar otro equipo e instalar aparte un IPS.

Siendo este (Snort) un equipo intermedio entre el Firewall y la infraestructura señuelo, debemos ejecutarlo en modo **INLINE (silencioso u oculto)**, de tal forma que sea transparente para un atacante y no pueda determinar su presencia o localización, para este efecto, las interfaces de conexión entre el Firewall y el Honeypot deben ser instalados en modo Bridge o puente (el cual trabaja en capa 2).

Aquí la configuración de las interfaces:

SNORT fue instalado en un sistema operativo UBUNTU 12.04, por lo cual la configuración de las interfaces se la realiza editando en el siguiente archivo:

vi /etc/network/interfaces

##
##

```
        # Loopback interface
auto lo
iface lo inet loopback
# Configurando el Bridge llamado br0
auto br0
iface br0 inet manual
# Puertos para adicionar en el Bridge, eth0 y eth1
   bridge_ports eth0 eth1
# Tiempo de espera antes de leer el Bridge = 0
bridge_maxwait 0
##################################################################
```

La topología de red quedará de la siguiente forma:

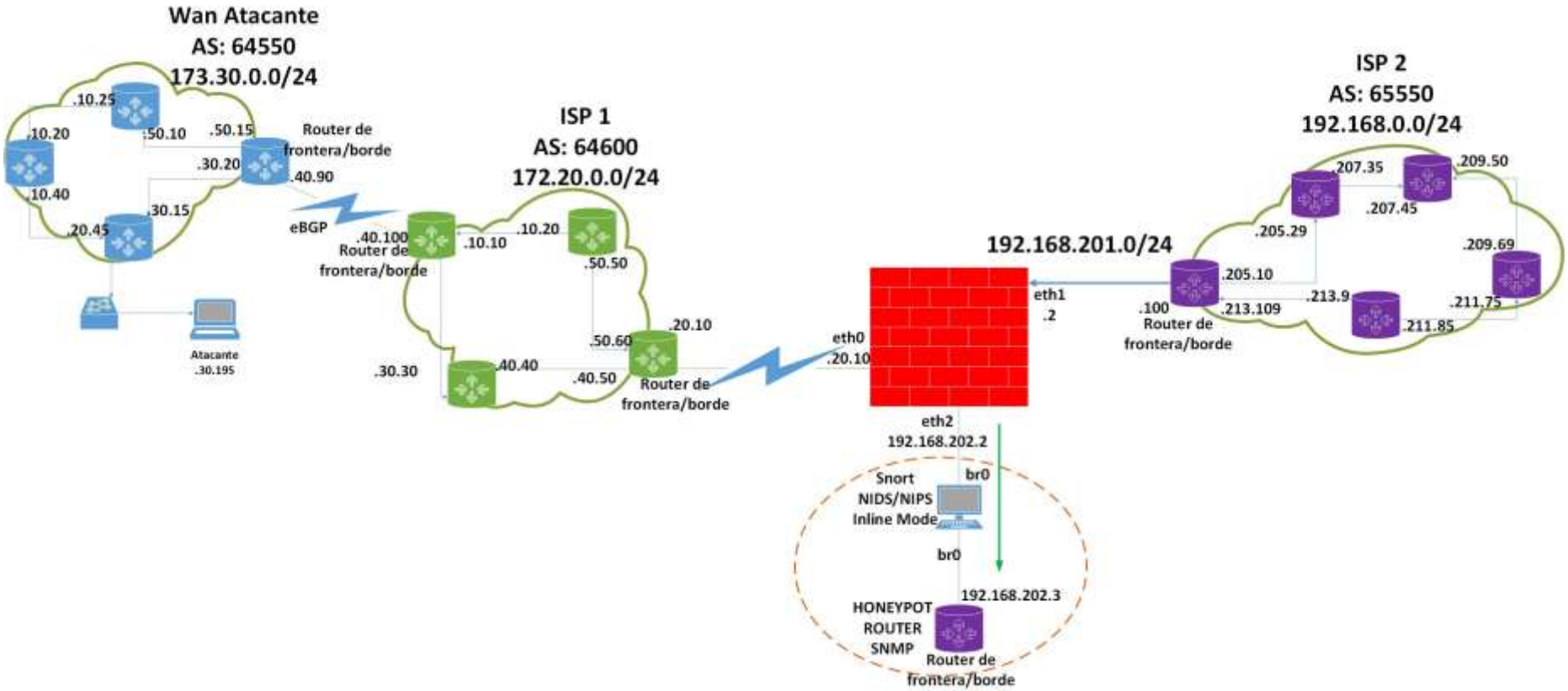


Figura 4-5: Infraestructura de Solución con detección y protección
Realizado por: Fabián Hurtado, 2016

Pruebas realizadas

Las pruebas fueron realizadas rigurosamente siguiendo las indicaciones de la fase 1 y 2, por lo que procedemos a mostrar la forma de detectar y analizar amenazas, tomando en cuenta el objeto de nuestro estudio, que es el HONEYPOT ROUTER. Los ataques realizados fueron:

Rastreo de puertos: este más que un ataque, es una de las fases más importantes que realiza todo atacante con/sin experiencia a la hora de realizar un pentesting, con la cual se determina el "vector de ataque" o en este caso, que puertos se encuentran abiertos, con el objetivo de asociar dicho puerto a un servicio dado, por lo que el ataque, de dar los resultados esperados, da pie o sirve de complemento a los otros 2 ataques a realizar, y por el hecho de NO crear consecuencias fatales a la infraestructura, se lo denomina un riesgo de nivel bajo.

El Escaneo de Puertos en la presente investigación se lo realiza de la siguiente manera:

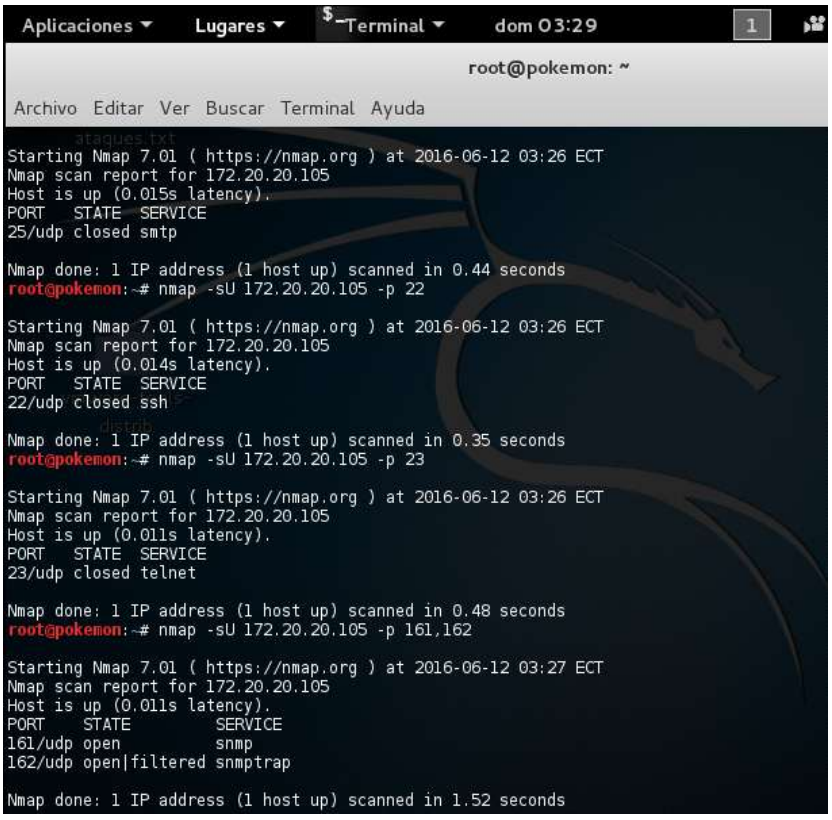


Figura 5-5: Ataque Rastreo de Puertos con NMAP
Realizado por: Fabián Hurtado, 2016

Aquí se muestra que mientras se realizaba un escaneo a los puertos que comúnmente se encuentran abiertos como el 23 TELNET, 25 SMTP, 22 SSH, según el resultado se encuentran cerrados, sin embargo, al escanear los siguientes puertos correspondientes al servicio SNMP 161 y 162, estos se encontraron abiertos y para hacerle seguimiento al escaneo realizado se ingresó a la aplicación Terminal, con el usuario ADMINISTRADOR "root" y ejecutamos el programa WIRESHARK, el cual se comporta como un Analizador de paquetes de red.

Luego se configura la interfaz de entrada por donde ingresaran los paquetes a ser analizados, en nuestro caso particular es la eth0.

De inmediato se ve que la herramienta comienza a capturar paquetes en la red:

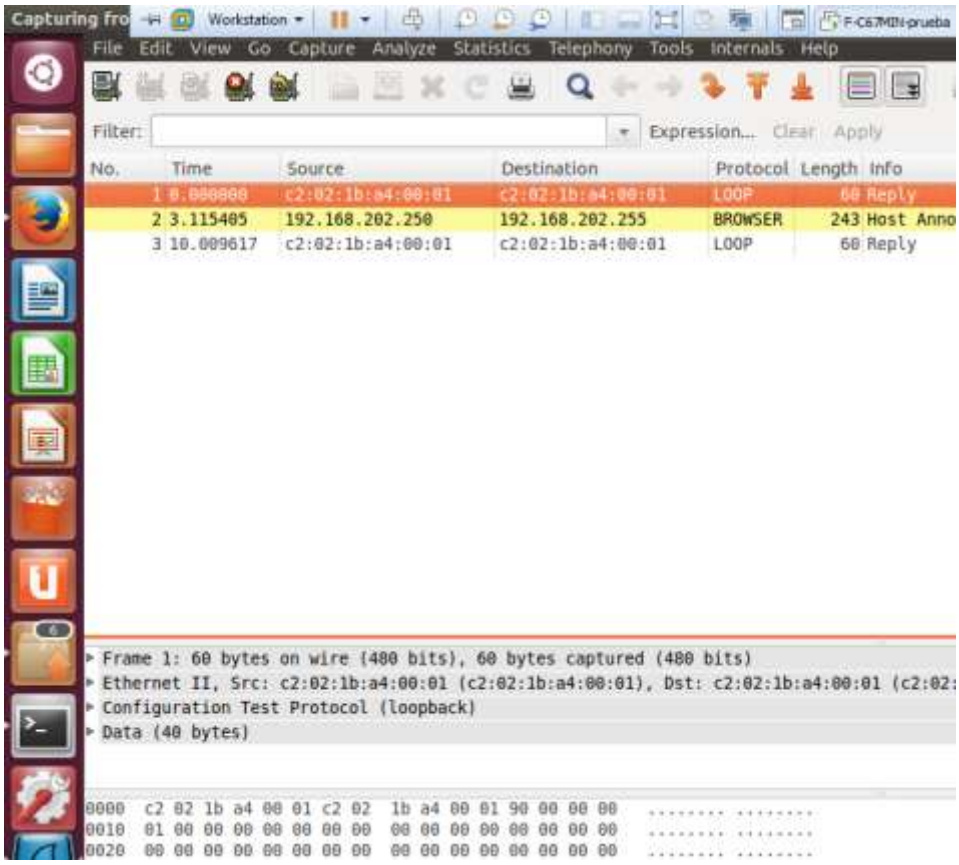


Figura 6-5: Captura de tráfico con la herramienta Wireshark
Realizado por: Fabián Hurtado, 2016

Al mismo tiempo que ejecuta WIRESHARK, también lo hará el Visualizador Web de SNORT IDS llamado ACIDBASE, desde el navegador que se tenga, ingresando a la página localhost/acidbase/base_main.php, el cual, y casi de inmediato comienza a detectar movimiento en la red, con la diferencia que en esta herramienta se deben crear las reglas de detección o también llamadas FIRMAS DE DETECCION.

Las firmas de detección se crean en el directorio /etc/snort/rules/ , aquí se almacenan todas las reglas para detección de "ingresos o peticiones no adecuadas". SRNOT desde su instalación ya trae reglas pre configuradas, incluyendo las del protocolo SNMP, pero al ser pre configuradas, solo están las que al parecer del desarrollador de la herramienta eran suficientes, aprovechándo eso y con la ayuda de un buen manual para conocer que significa cada comando, (Snort, 2013) se procede a adicionar firmas propias, de acuerdo al análisis previamente realizado en el WIRESHARK.

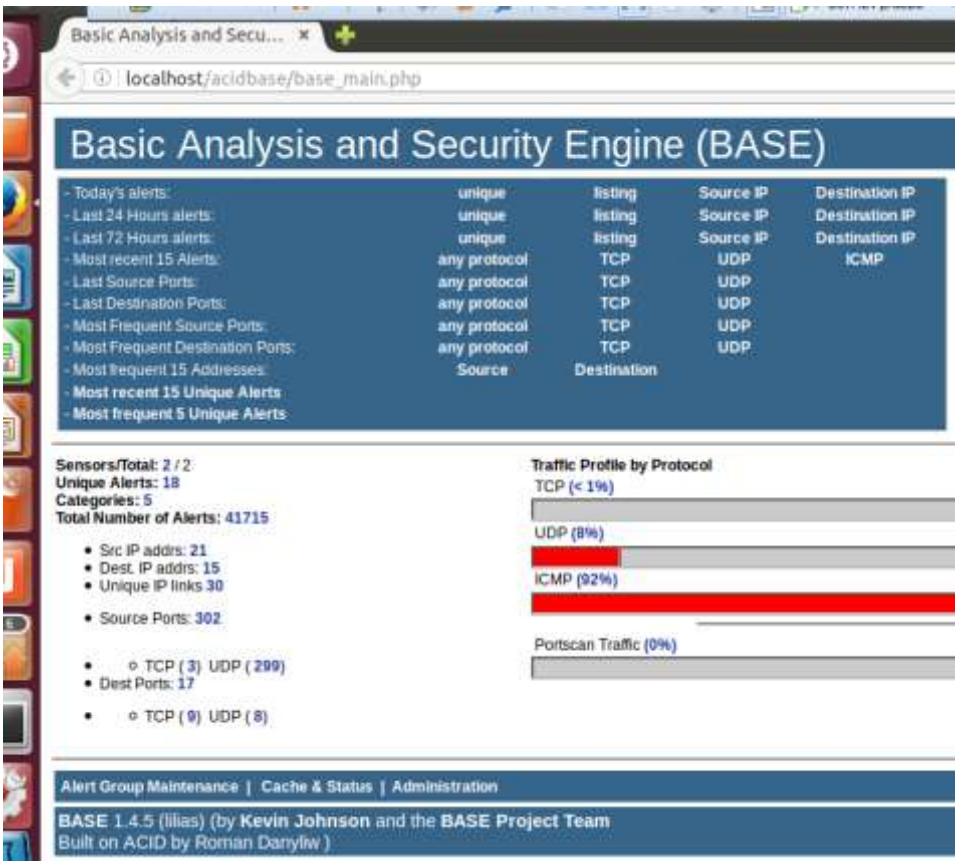


Figura 7-5: Visualizador ACIDBASE web
Realizado por: Fabián Hurtado, 2016

Como se comentó en párrafos anteriores, se realizó el ataque ESCANEO DE PUERTOS con la herramienta instalada en la suite KALI LINUX 2.0 llamada NMAP ver 7.0.

Nmap es un programa de código abierto que sirve para efectuar rastreo de puertos escrito originalmente por Gordon Lyon (más conocido por su alias Fyodor Vaskovich) y cuyo desarrollo se encuentra hoy a cargo de una comunidad. Fue creado originalmente para Linux aunque actualmente es multiplataforma. Se usa para evaluar la seguridad de sistemas

informáticos, así como para descubrir servicios o servidores en una red informática, para ello Nmap envía unos paquetes definidos a otros equipos y analiza sus respuestas.

Este software posee varias funciones para sondear redes de computadores, incluyendo detección de equipos, servicios y sistemas operativos. Estas funciones son extensibles mediante el uso de scripts para proveer servicios de detección avanzados, detección de vulnerabilidades y otras aplicaciones. Además, durante un escaneo, es capaz de adaptarse a las condiciones de la red incluyendo latencia y congestión de la misma. Una característica propia de la aplicación es asegurarse de que el objetivo este en pleno funcionamiento, por lo cual, a parte de enviar el paquete escaneador del puerto, también envía un paquete ICMP.(Nmap, 2016b).

Teniendo las 2 herramientas corriendo, se realiza nuevamente el ataque utilizando NMAP, con el siguiente comando:

#nmap –sU 172.20.20.105 –p 161,162

La opción **–sU** significa que se va a escanear el **protocolo UDP.**
La opción **–p** permite identificar el número de puerto que se desea escanear.

Al analizar el resultado que se observa en la herramienta WIRESHARK y teniendo en cuenta que no van a mostrarse solo el ataque realizado sino, todos los paquetes que en ese momento están circulando por la red, se tendría que aplicar un filtro para solo visualizar lo que se desea, que es el paquete del escaneo NMAP directo al protocolo SNMP protocolos 161, 162.

Las transmisiones normales de comandos SNMP manejan el puerto 161 y los TRAPS SNMP o mensajes críticos de cambio de estado de un proceso de administración se manejan en el puerto 162.

El primer filtro que creamos es el siguiente:
ip.addr ==173.30.30.195 and snmp.
Luego se aplica el cambio al filtro en **Apply**

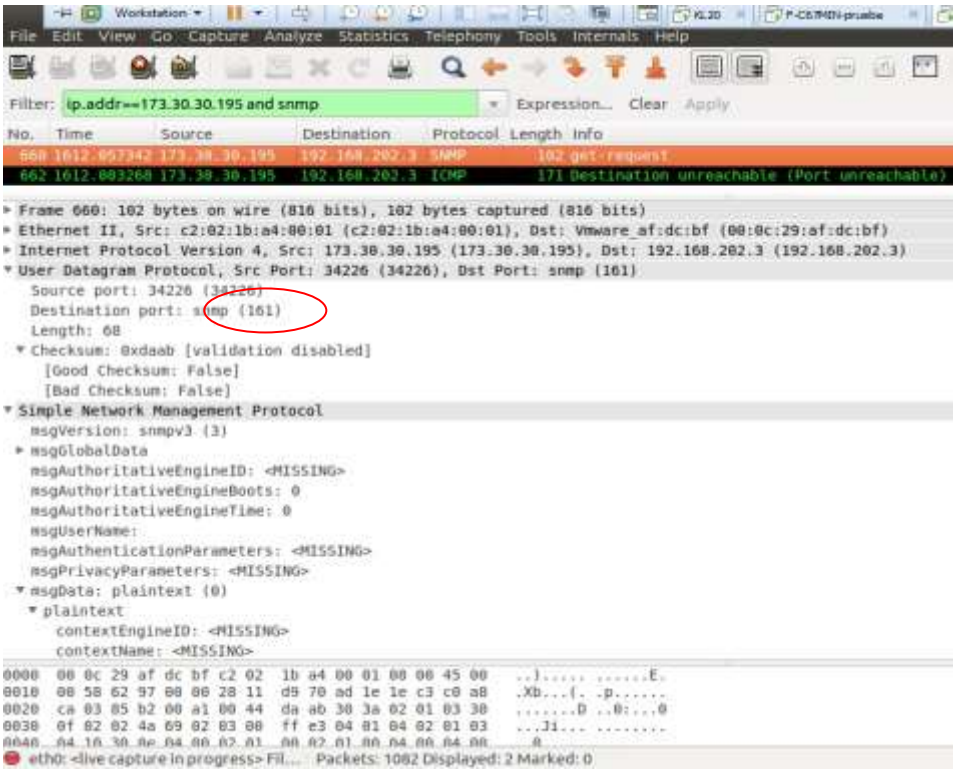


Figura 8-5: Vista de protocolo SNMP en ataque
Realizado por: Fabián Hurtado, 2016

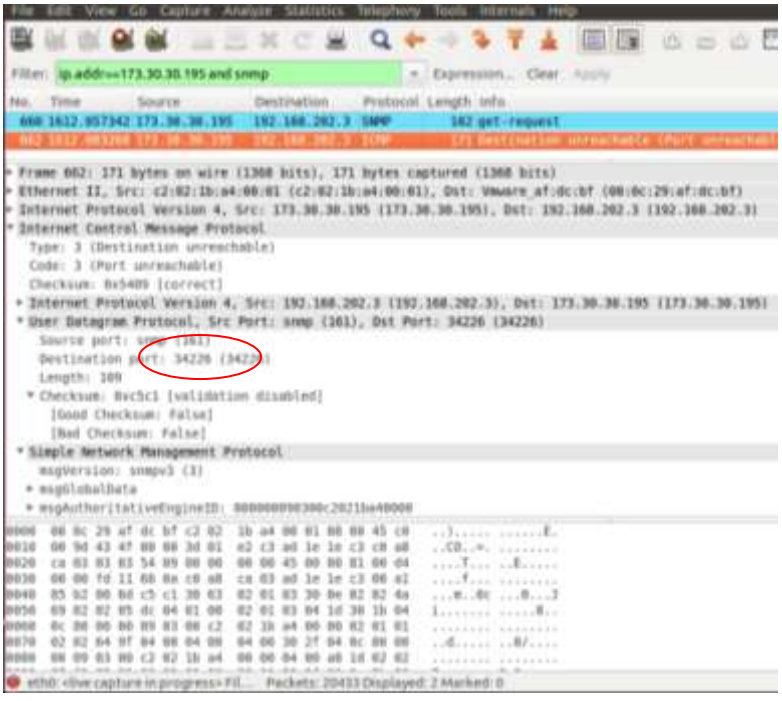


Figura 9-5: Vista del protocolo ICMP en ataque
Realizado por: Fabián Hurtado, 2016

Ya que UDP no es un protocolo orientado a conexión como TCP, la única respuesta que podíamos recibir del puerto objetivo, era un mensaje de ICMP Port Unreacheable, esto se da

debido a que existe algún dispositivo de por medio tratando de detener paquetes desconocidos o no permitidos como un firewall.(Operating System and Service detection - Nicholas March, 2010)

Como se indicó anteriormente, este cambio fue lanzado por completo en la versión 6.0 del 21-jul-2012 tal como lo indica su sitio web.(Nmap, 2016a)

El siguiente filtro que se aplica es sobre los TRAPs de SNMP.

ip.addr ==173.30.30.195 and udp.port == 162

Luego se aplica el cambio al filtro en **Apply**

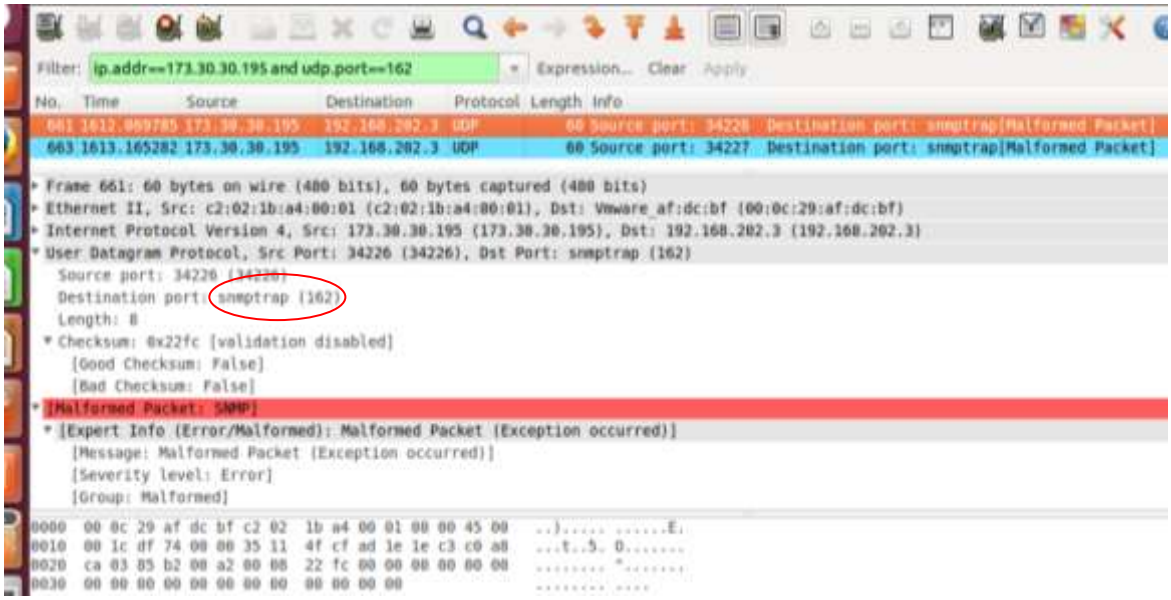


Figura 10-5: Detalle del puerto 162 snmptrap
Realizado por: Fabián Hurtado, 2016

Dado que el paquete no está llevando ningún tipo de información, se muestra como "malformado". Ahora que se conocen que puertos están comprometidos se debe fabricar la firma para detección de todas las amenazas que tengan este parámetro, con esto, el SNORT - IDS podrá reconocer cuando hay un requerimiento a los 2 puertos (161 y 162) por medio del software NMAP.

Algo muy importante que hay que tomar en cuenta que esta es una infraestructura ISP tradicional, por lo que para la presente investigación, con el objetivo de filtrar paquetes SNMP se instala un FIREWALL, ya que se necesita un dispositivo que pueda leer atreves de puertos en

capa 4, y en esta infraestructura WAN se tienen publicados servicios de monitoreo de red, en este caso SNMP

Se escoge el archivo snmp.rules del directorio /etc/snort/rules/ para colocar nuestras reglas.

Este archivo de reglas pre configurado se encuentra ya registrado en el /etc/snort/snort.conf

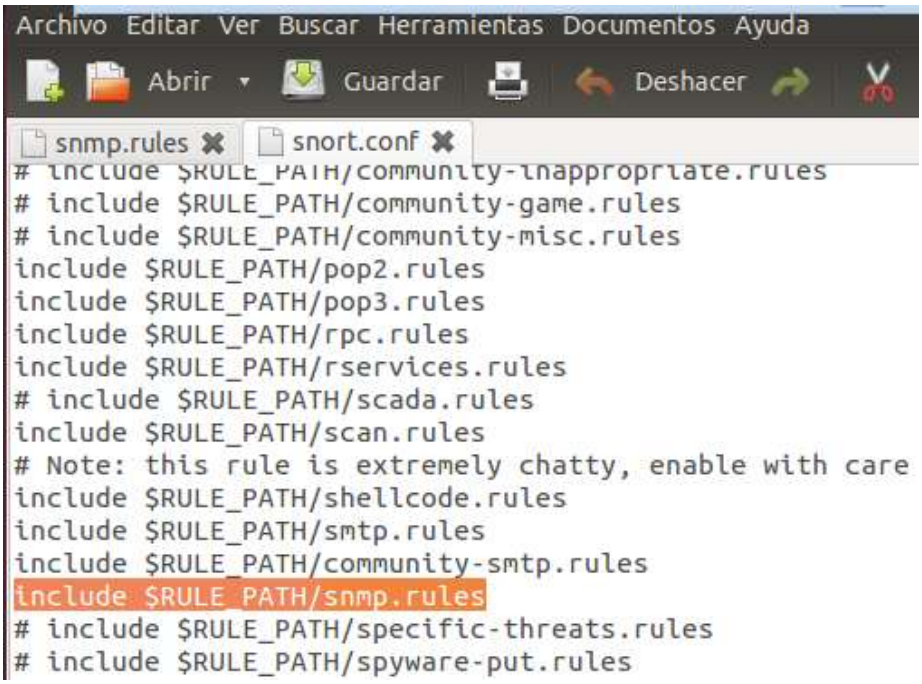


Figura 11-5: Archivo de reglas o firmas
Realizado por: Fabián Hurtado, 2016

La regla a aplicar en el archivo .rules es la siguiente.

Alert udp $EXTERNAL_NET any -> $HOME_NET 161 (content:"|30 3A 02 01 03 30 0F 02 02 4A 69 02 03 00 FF E3|";msg:"NS-ATQUE SNMP 161 request udp"; classtype:network-scan; sid:1417; rev:9;)

Se procede a explicar punto por punto:

Alert: Acción de la regla, de tipo alerta

Udp: protocolo a analizar

$EXTERNAL_NET: variable que contiene la dirección ip o de red en este caso la EXTERNA configurada en el archivo /etc/snort/snort.conf

Any: Puerto de origen de la variable $EXTERNAL_NET

->: indica la dirección u orientación para aplicar la regla en este caso desde la Externa hacia la Home

$HOME_NET: variable que contiene la dirección ip o de red en este caso la Interna o Home configurada en el archivo /etc/snort/snort.conf

161: número del puerto analizar

content:"|30 3A 02 01 03 30 0F 02 02 4A 69 02 03 00 FF E3|" : Contenido en particular que se encuentra dentro del paquete analizado, el cual, puede servir para diferenciarlo de ataques tipo FALSOS POSITIVOS de uno que sea REAL.

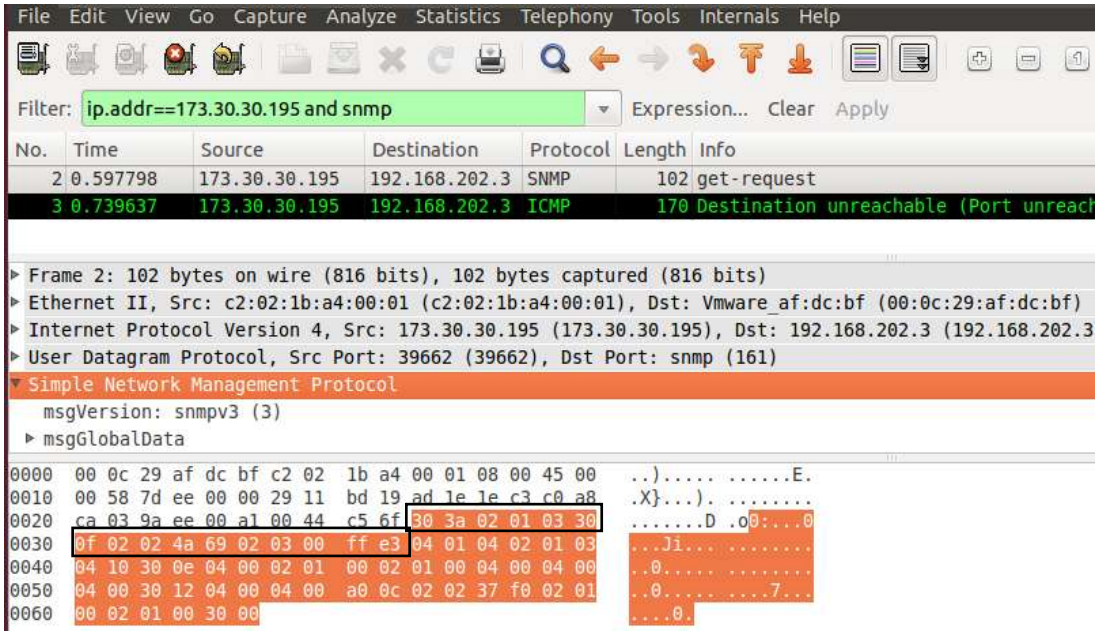


Figura 12-5: Contenido hexadecimal particular
Realizado por: Fabián Hurtado, 2016

msg:"NS- ATQUE SNMP 161 request udp": Mensaje que aparece apenas se analice el ataque. NS significa NETWORK SCAN.

classtype:network-scan: categorización de la regla, de acuerdo al listado en el anexo A3, tiene una prioridad baja.

sid:1417 : Snor ID, código de identificación de SNORT

rev:9 : número de revisión de la regla (número aleatorio)

Con esta regla ingresada y guardada, en el nuevo ataque nmap hacia snmp el SNORT-IDS lo detectará y mostrará el siguiente mensaje en su sistema de visualización ACIDBASE conectado al motor de Detección.

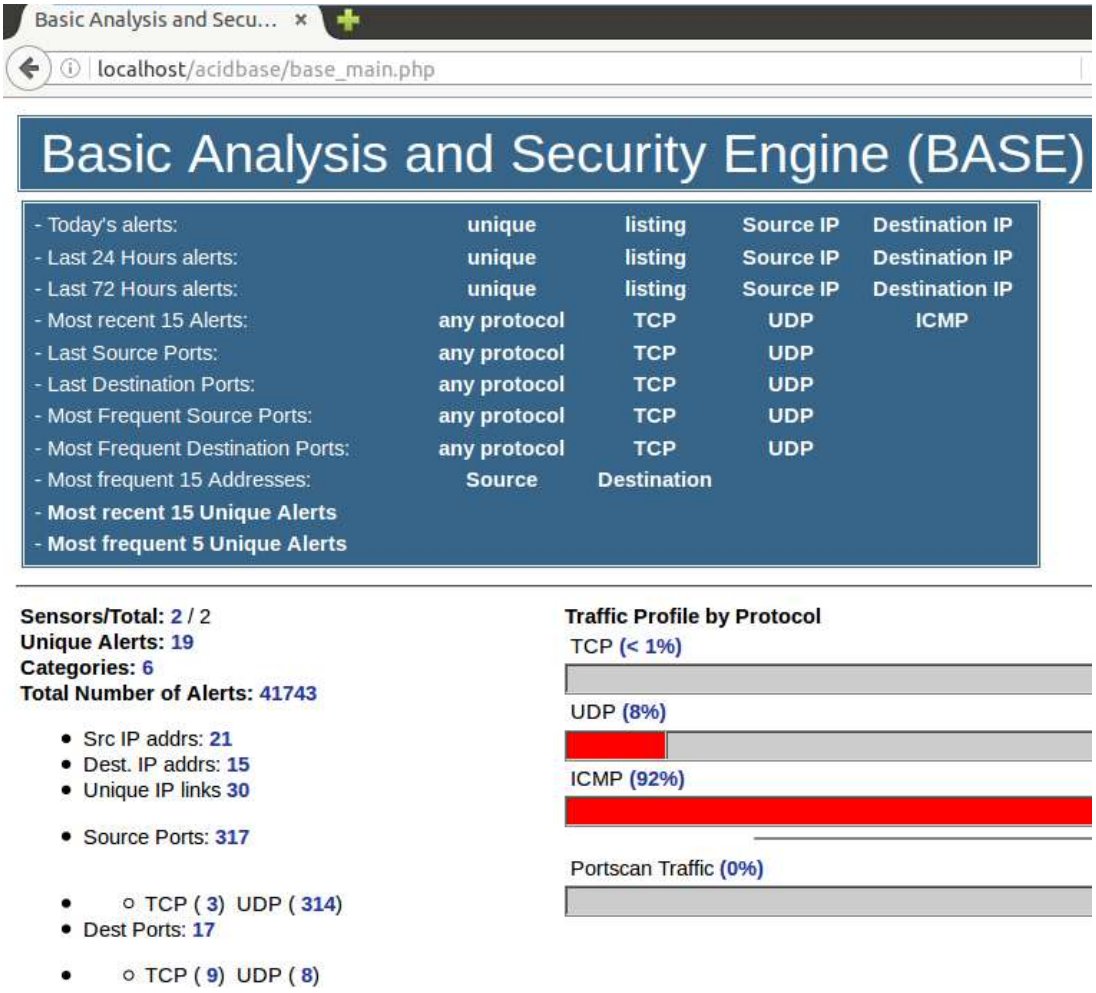


Figura 13-5: ACIDBASE visualizando nuevo ataque detectado
Realizado por: Fabián Hurtado, 2016

Ingresando en el 8% de los paquetes UDP tenemos lo siguiente:

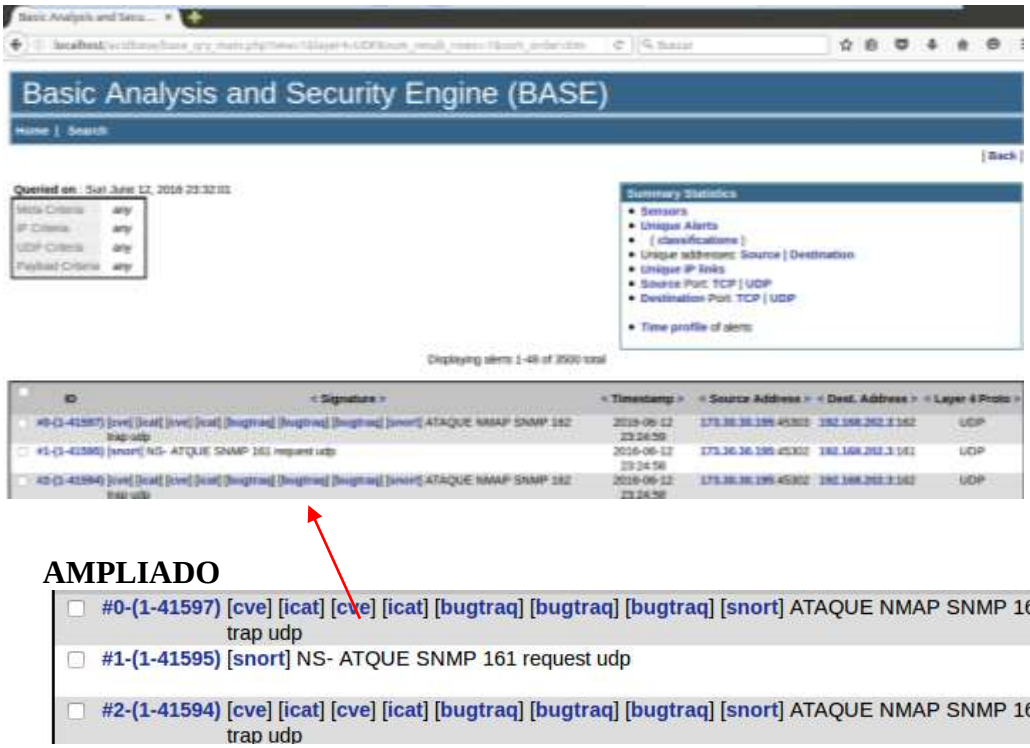


Figura 14-5: Ataque detectado con SNORT - IDS
Realizado por: Fabián Hurtado, 2016

Como se puede visualizar, también aparece un mensaje para el puerto UDP 162, el cual su configuración en el archivo de reglas es el siguiente:

Alert udp $EXTERNAL_NET any -> $HOME_NET 162 (msg:"ATAQUE NMAP SNMP 162 trap udp"; classtype:network-scan; sid:1419; rev:9;).

Aunque el puerto no lleva ninguna información de relevancia TRAP, no se puede dejar de configurar una regla (aunque sea para que se note que también se está solicitando un NMAP al puerto 162), ya que en SEGURIDAD INFORMATICA NADA PUEDE SUPONERSE QUE NO VA A OCURRIR.

En lo referente al consumo de cpu y memoria del HONEYPOT-ROUTER, es la siguiente:

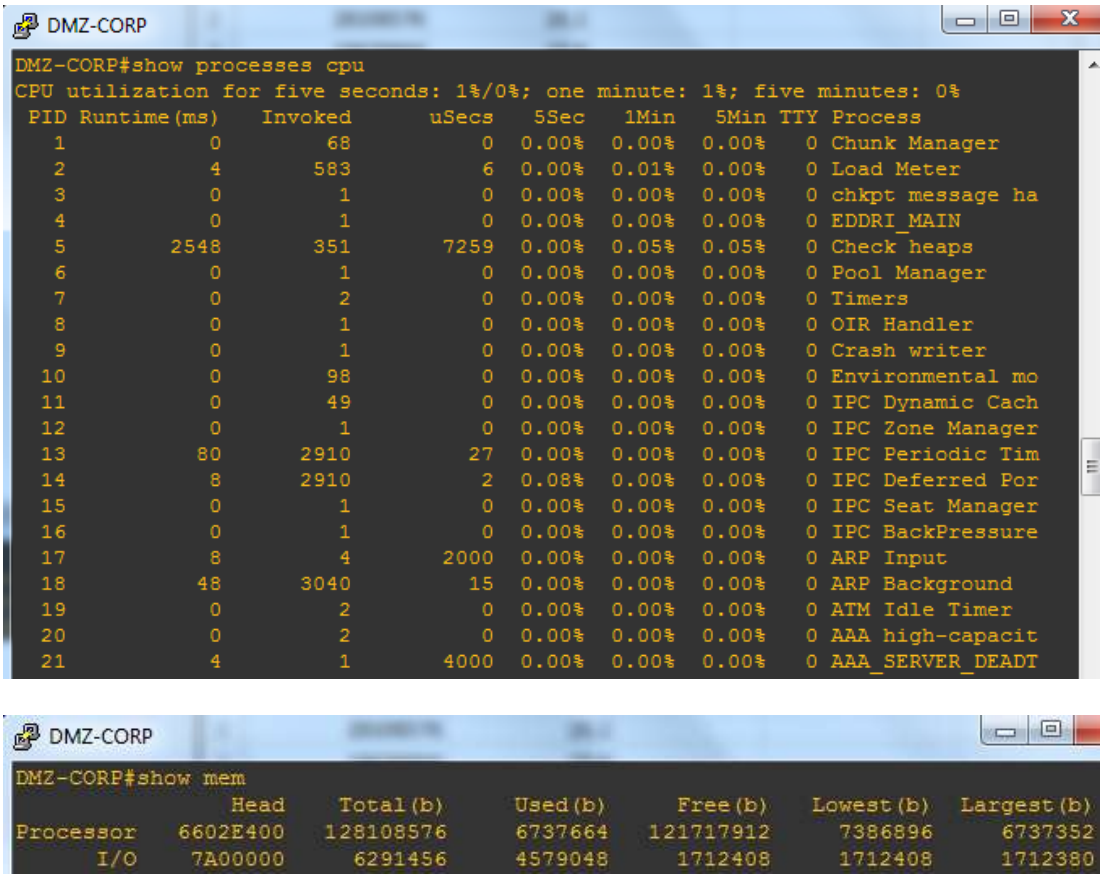


Figura 15-5: Performance del CPU y Memoria durante ataque escaneo de puertos
Realizado por: Fabián Hurtado, 2016

Consumo del procesador 1% y de la memoria es de 5,2% (6,7 mb)

Ahora se procede a detectar un ataque de **FUERZA BRUTA O DICCIONARIO**, el cual es realizado partir de la información proveída por NMAP, al indicarnos que el protocolo SNMP está abierto y disponible.

El ataque será realizado con la herramienta llamada snmp-brute, programada y disponible para todas las distribuciones Linux que tengan instalado el lenguaje Python.

De acuerdo a la ISO 27001, un ataque de diccionario o fuerza bruta es un método de cracking/romper que consiste en intentar averiguar una contraseña probando todas las palabras de un diccionario. (Honan, B., 2010)

Los ataques de fuerza bruta tienen pocas probabilidades de éxito con sistemas que emplean contraseñas fuertes con letras en mayúsculas y minúsculas mezcladas con números (alfanuméricos) y con cualquier otro tipo de símbolos. Sin embargo, para la mayoría de los

usuarios recordar contraseñas tan complejas resulta complicado. Existen variantes que comprueban también algunas de las típicas sustituciones (determinadas letras por números, intercambio de dos letras, abreviaciones), así como distintas combinaciones de mayúsculas y minúsculas.

El ataque es más efectivo mientras más completo sea el diccionario, y mientras más completo es más pesado se vuelve por la cantidad de combinaciones alfanuméricas que tiene, ya que al momento de encontrar el cifrado correcto o la contraseña adecuada, la seguridad del sistema se rompe de forma brutal, o sea muy rápido o muy lento.

Los sistemas que ya existen para este tipo de ataques son entre otros:

Crack de Alec Muffett
John the Ripper
L0phtCrack
Cain
Medusa
Cisc0wn
Hydra
afp-brute
domcon-brute
drda-brute
ftp-brute
http-brute
http-form-brute
informix-brute
iscsi-brute
ldap-brute
ms-sql-brute
mysql-brute
netbus-brute
oracle-brute
oracle-sid-brute
pgsql-brute
pop3-brute
smb-brute

snmp-brute
svn-brute
telnet-brute
vnc-brute

En este caso particular, lo que se intentará adivinar y romper es el String de la comunidad SNMP RW de un equipo Cisco administrado, usando un diccionario. Las comunidades SNMP RW se comunican entre sí para poder proceder desde el manager con los comandos get, set. El programa snmp-brute es el escogido para realizar el ataque por estar totalmente direccionado al puerto UDP 161, con los comandos correctos y dirigidos a los OID's correspondientes.(Nmap, 2012).

Una vez determinado cual es el string, el mismo, nos da informaciones en pantalla de las configuraciones, tablas de enrutamiento, entre otros, en el caso de los equipos Cisco. Adicional a esto invoca Metasploit con su respectivo módulo para descargar la configuración del equipo y en caso de encontrar passwords en texto plano los muestra en pantalla, de estar cifrados (no estén en texto plano) intenta crackearlos invocando John the Ripper.

Las dependencias o programas complementarios para que snmp-brute funciones son lo siguientes:

- Metasploit
- Snmpstat
- Snmpwalk
- John The Ripper

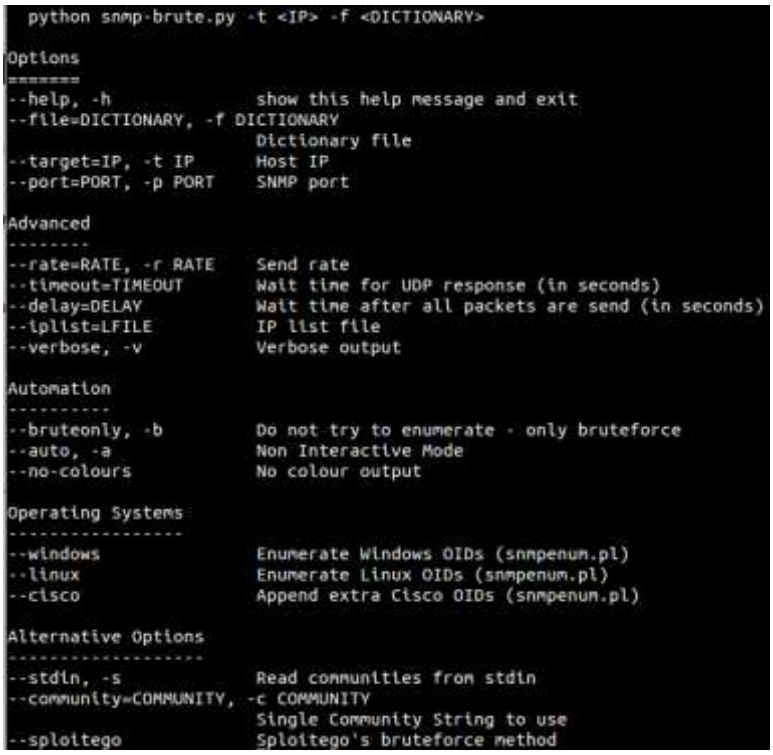


Figura 16-5: Opciones del programa snmp-brute.py
Realizado por: Fabián Hurtado, 2016

El ataque fue concebido de la siguiente manera:
Invocando a Python desde Kali Linux:

python snmp-brute.py –t 172.20.20.105 –f snm1.txt

Donde 172.20.20.105 es la dirección ip atacada y snm1.txt el diccionario que se va a utilizar para los intentos de fuerza bruta.

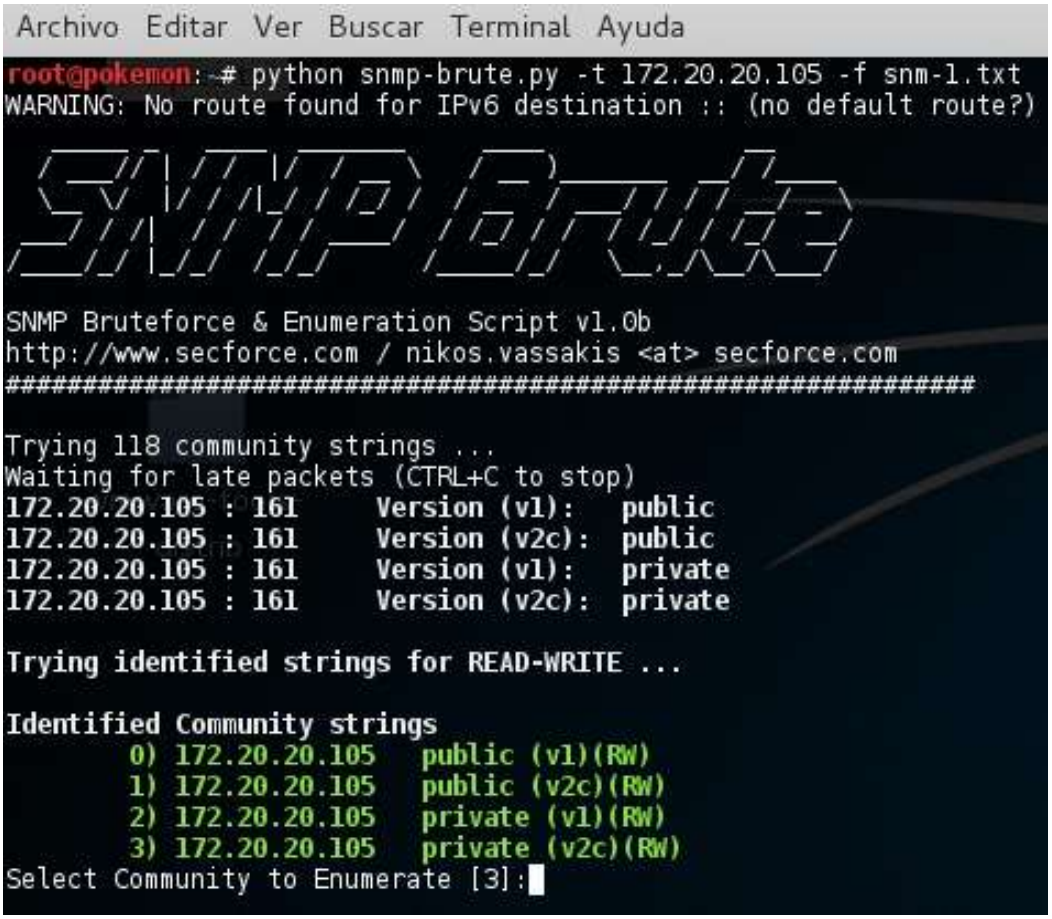


Figura 17-5: Ataque de Fuerza Bruta hacia SNMP
Realizado por: Fabián Hurtado, 2016

Aquí se muestra el trabajo realizado por snmp-brute teniendo un buen diccionario dedicado a adivinar la seguridad de la comunidad SNMP RW, el programa envía paquetes Get-Request al puerto 161 de la dirección 172.20.20.105 del Firewall teniendo éxito y las comunidades RW encontradas fueron la "public" - "private", también le da al atacante la información sobre que versión del protocolo SNMP podría estar corriendo en ese momento.

Debido a que en el código programado, el ataque va dirigido a obtener el valor String del sysContact o comunidad SNMP WR, su código OID en la MIB II es : .1.3.6.1.2.1.1.4.0, tal como se lo ve en la Figura 18-5 que muestra parte del programa:

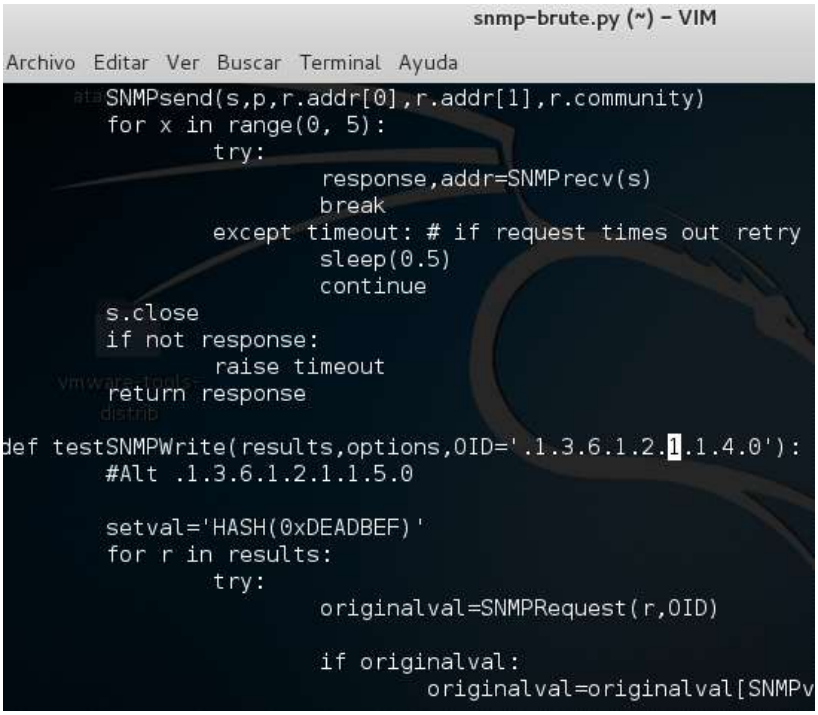


Figura 18-5: Edición del programa snmp-brute.py
Realizado por: Fabián Hurtado, 2016

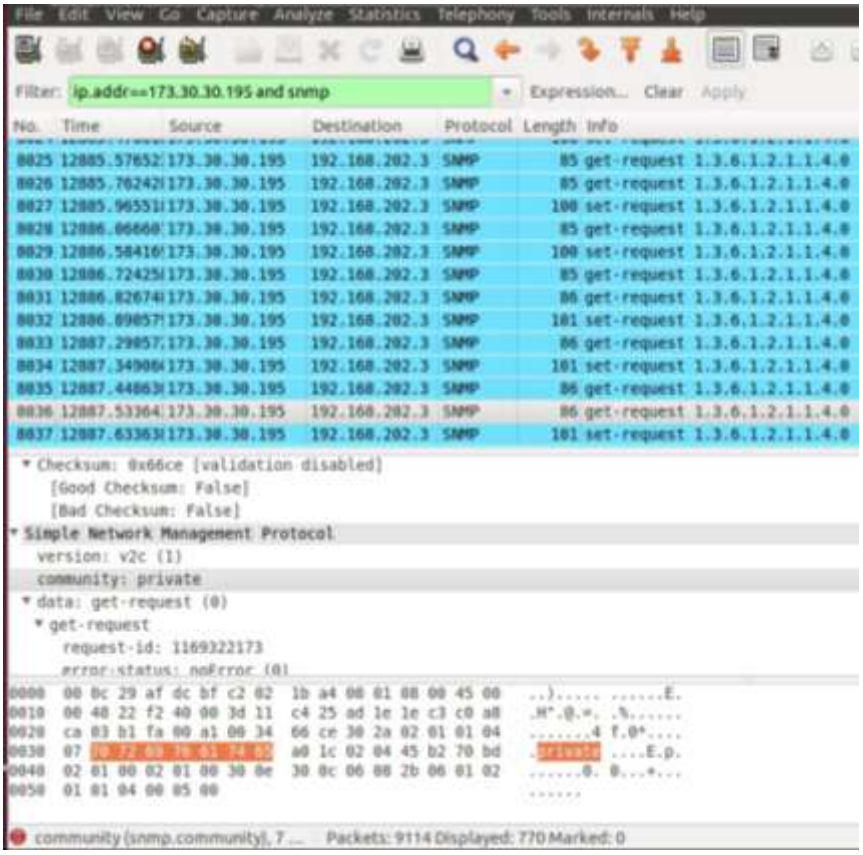


Figura 19-5: String "private" encontrado por diccionario
Realizado por: Fabián Hurtado, 2016

En la Figura 19-5 se puede observar el ataque en WIRESHARK, y como después de varios intentos por obtener el String por medio del diccionario, aparece la palabra “private”, así mismo aparece la palabra “public”, ya con esto se puede armar la regla de detección en el Snort-IDS

alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"Intento Acceso SNMP 161 public udp"; content:"public"; classtype:attempted-recon; sid:1411; rev:10;)

alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"Intento Acceso SNMP 161 private udp"; content:"private"; classtype:attempted-recon; sid:1413; rev:10;)

Con estas reglas aplicadas en el IDS, se observa el ataque realizado mediante el Visualizador del Snort-IDS, nótese los diferentes mensajes que aparecerán para los ataques hacia la comunidad “public” y “private”

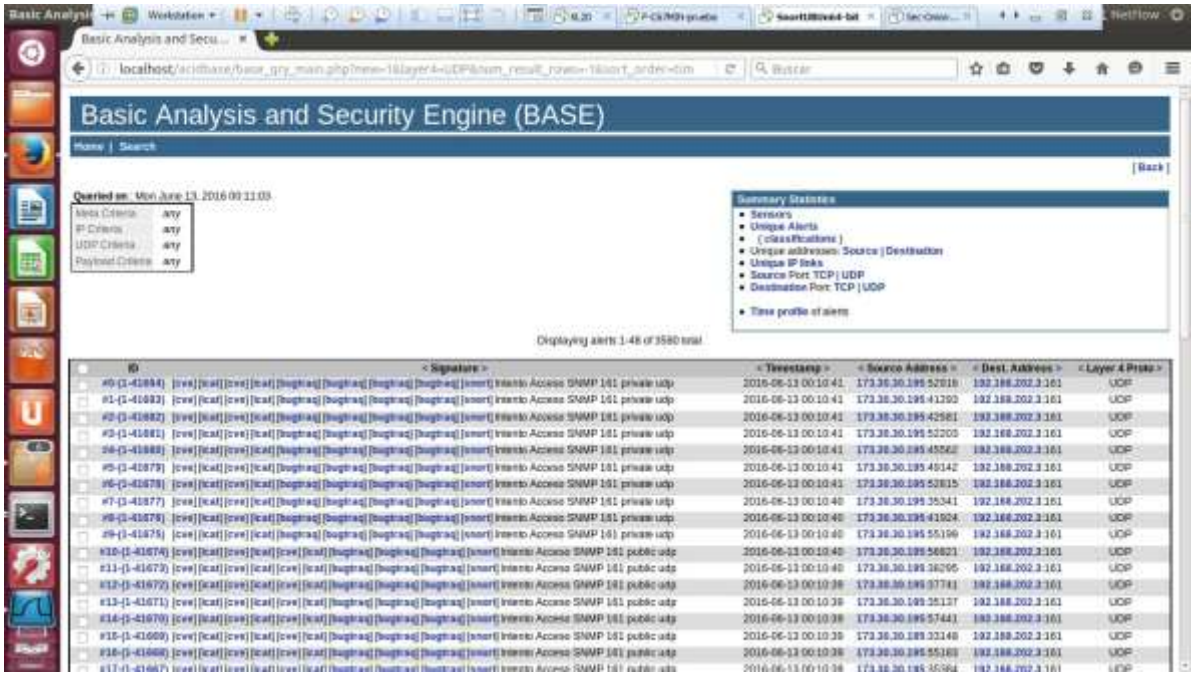
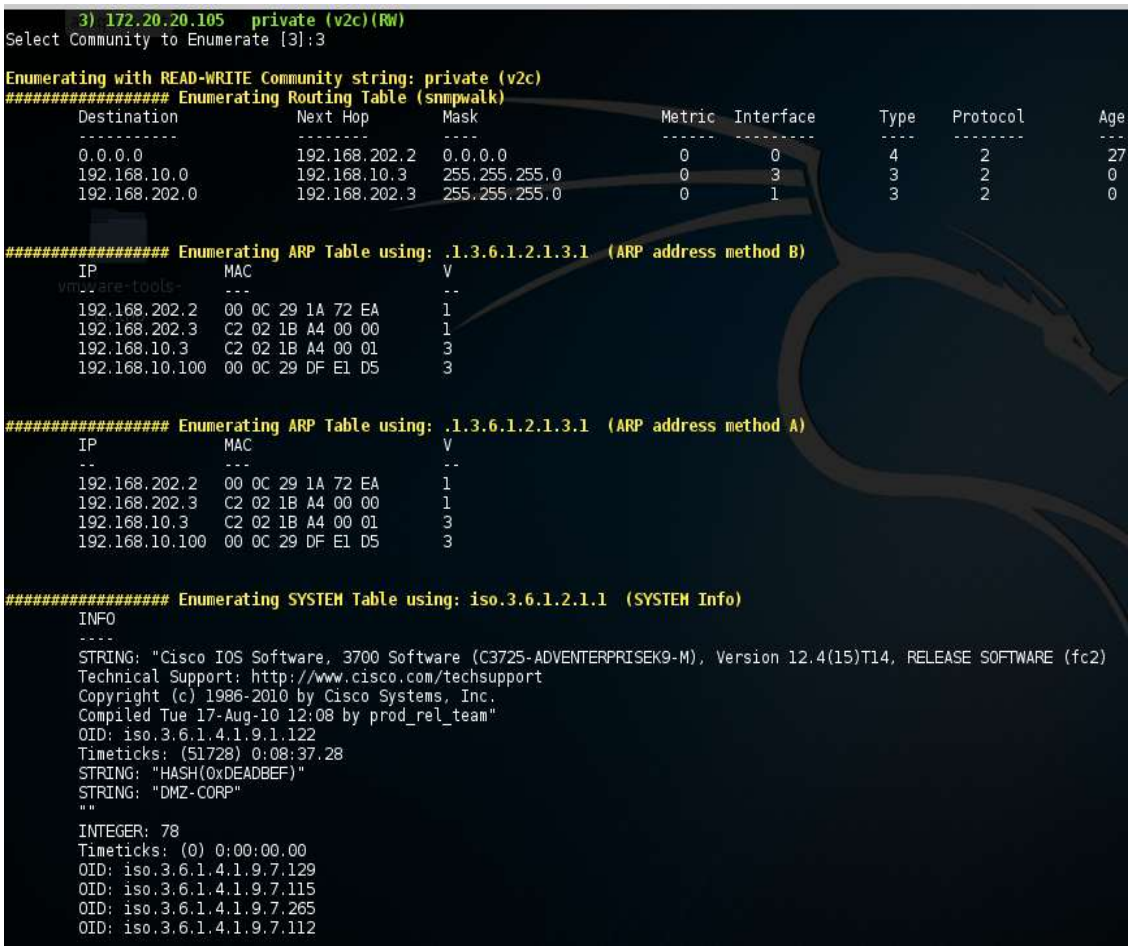


Figura 20-5: Comunidades "private" y "public" encontradas
Realizado por: Fabián Hurtado, 2016

Continuando con el desarrollo del programa snmp-brute, luego de encontrar las comunidades SNMP RW hábiles, al atacante le aparece una ayuda, indicando que numero a escoger para complementar el ataque de diccionario extrayendo toda la MIB del objeto administrado, en este

caso la ayuda es para realizar el ataque con la opción **[3]** y se observara lo que ocurre tanto en WIRESHARK y SNORT/IDS.



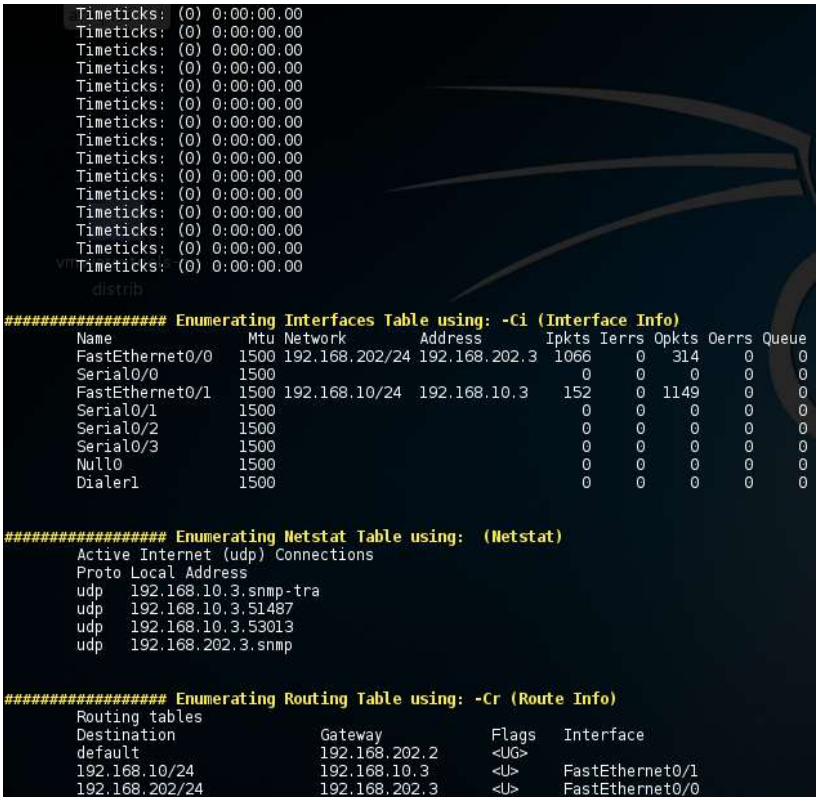


Figura 21-5: Opción 3 extrayendo el detalle del Router atacado
Realizado por: Fabián Hurtado, 2016

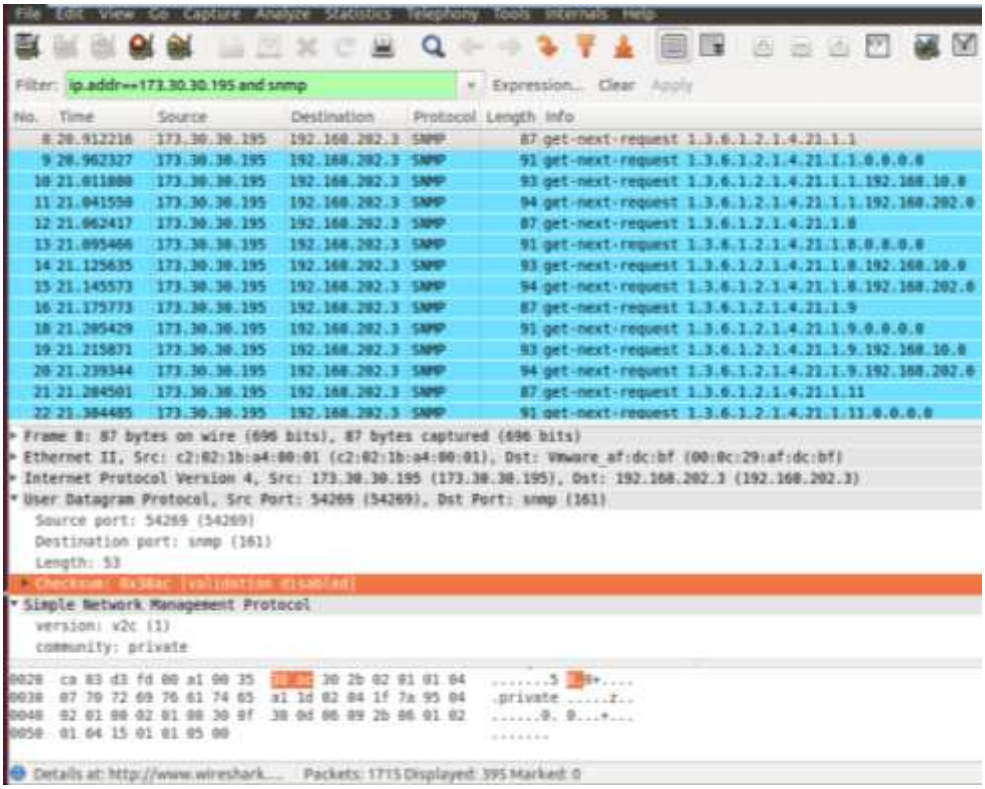


Figura 22-5: Muestra por Wireshark de la extracción
Realizado por: Fabián Hurtado, 2016

Al haber escogido la opción 3 toda la extraccion de datos se dara por medio de la comunidad "private", activando la regla de alerta antes creada. Si se hubiera escogido la opción 0 o 1 toda la extraccion de datos se daría por medio de la comunidad "public", activando la regla respectiva.

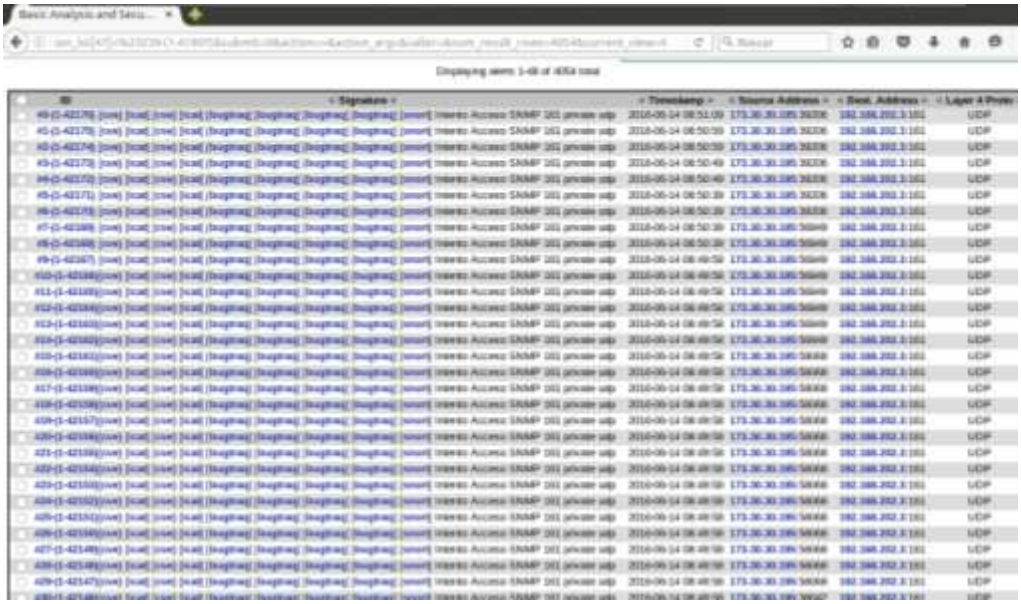


Figura 23-5: Visualización con ACIDBASE de la extracción
Realizado por: Fabián Hurtado, 2016

Tambien hay que tomar en cuenta el performance del router, midiendo la utilizacion de la CPU y la memoria. Aquí una imagen del mismo.

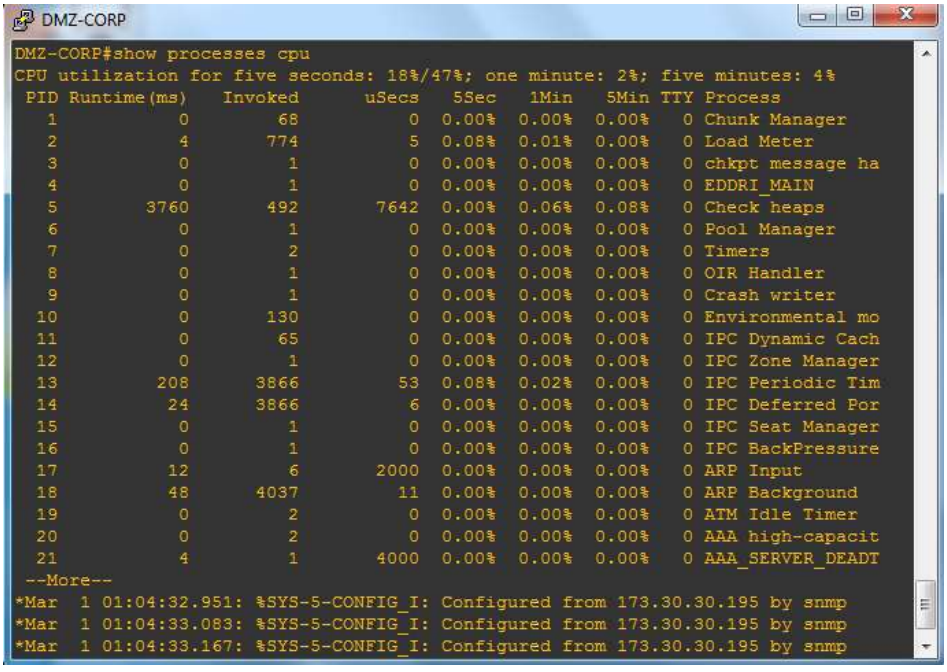


Figura 24-5: Performance del CPU del Router atacado
Realizado por: Fabián Hurtado, 2016

Con esto se prueba que mientras hubo este ataque, el Router tuvo una utilización de la CPU en 5sgds. de 18%, 1 minuto del 2% con un maximo de 4% en 5 minutos, del Router de Frontera llamado DMZ, lo cual no es considerable.

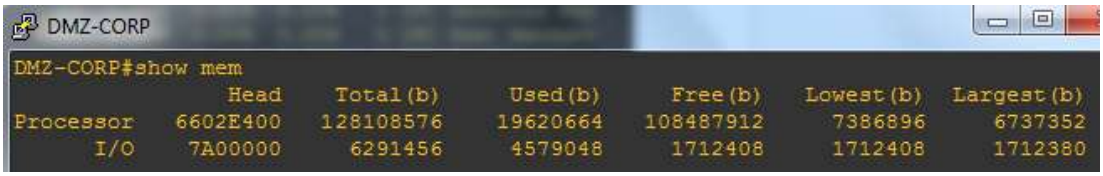


Figura 25-5: Performance de la memoria del Router de Frontera atacado
Realizado por: Fabián Hurtado, 2016

En lo que se refiere a memoria tampoco es considerable el consumo 21,12 mb (16,50%), tomando en cuenta que los equipos tienen una memoria de 128 Mb.

Ahora se procederá a detectar un ataque de **DENEGACIÓN DE SERVICIOS DISTRIBUIDO**, el cual es realizado partir de la información proveída por NMAP y snmp-brute (escaneo de puertos y fuerza bruta), al indicar que el protocolo SNMP está abierto y disponible con las comunidades "private" y "public"

El ataque será realizado con la herramienta llamada snmp-DDOS, programada y disponible para todas las distribuciones Linux que tengan instalado el lenguaje Python.(Security By Default, 2014)

Primero se procede a explicar que es y cómo funciona un ataque de DDoS, según el RFC4732, CISCO y el Computer Emergency Response Teams (CERT) (Handley, M. J., & Rescorla, E., 2006), (Cisco Systems, 2010a), (US-CERT, 2012)

DDoS son las siglas de Distributed Denial of Service, la traducción es "ataque de denegación de servicio distribuido", y traducido de nuevo significa que se ataca al servidor/surtidor de servicios desde muchos ordenadores para que deje de funcionar el mismo, pero aun así esto no guía mucho sobre lo que es un DDoS, para una mejor comprensión se procede con una simple analogía en la que el servidor es un cajero bancario que atiende a personas en una ventanilla.

El cajero es muy eficiente y es capaz de atender a varias personas a la vez sin despeinarse: es su carga normal. Pero un día empiezan a llegar cientos de personas a la ventanilla a pedirle cosas al cajero. Y como cualquier humano normal, cuando hay mucha gente con más trabajo de lo

habitual no puede atender a todos y empieza a realizar sus tareas más lento de lo normal. Si viene todavía más gente probablemente se enferme, se marchará de la ventanilla y ya no atenderá a nadie más.

En el servidor/surtidor de servicios pasa lo mismo: cuando hay demasiadas peticiones se queda sin recursos, se cuelga y deja de funcionar. Puede que se apague directamente o que sólo deje de responder conexiones. De cualquiera de las dos formas, el servidor no volverá a la normalidad hasta que el ataque pare, ya sea porque los atacantes se han detenido o porque se logrado bloquear las conexiones ilegítimas, y se rearranque todo lo que haya dejado de funcionar.

Este es el concepto básico del DDoS, aunque se puede modificar para que sea más efectivo. Por ejemplo, se pueden enviar los datos muy lentamente haciendo que el servidor consuma más recursos por cada conexión (Slow Read es un ejemplo de ataque de este tipo), o alterar los paquetes para que el servidor se quede esperando indefinidamente una respuesta de una IP falsa (el nombre técnico es SYN flood).

Como el concepto básico del DDoS es simple, realizar los ataques es relativamente fácil. De hecho, valdría con que hubiese un número suficientemente grande de personas recargando la web continuamente para tirarla abajo. Sin embargo, las herramientas que se suelen usar son algo más complejas.

Con ellas se pueden crear muchas conexiones simultáneas o enviar paquetes alterados con las técnicas antes comentadas. También permiten modificar los paquetes poniendo como IP de origen una IP falsa, de forma que no pueden detectar quién es el atacante real.

Otra técnica para llevar a cabo los DDoS es usar botnets: redes de ordenadores infectados por un troyano y que un atacante puede controlar remotamente. De esta forma, los que saturan el servidor son ordenadores de gente que no sabe que están participando en un ataque DDoS, por lo que es más difícil encontrar al verdadero atacante. Cuando el servidor de servicios se satura deja de estar disponible durante un tiempo hasta que el ataque para. Es muy difícil que se produzcan daños físicos en el servidor. Además, el ataque DDoS por sí sólo no permite entrar en el servidor: para ello es necesario aprovechar alguna vulnerabilidad, y eso no es nada fácil.

De acuerdo a la investigación propuesta, el objetivo es realizar un ataque de denegación de servicio distribuido aprovechando las vulnerabilidades que nos brinda el protocolo SNMP, el escaneo de protocolos con NMAP y el ataque de fuerza bruta realizado con anterioridad.

Antes de entender la técnica de DDoS realizada a un protocolo SNMP (Security By Default, 2014), hay recordar que SNMP es un protocolo de administración, su uso ha sido muy extendido para el monitoreo y supervisión de los dispositivos de red en entornos corporativos, existen tres versiones SNMP v1, v2c y v3, las dos primeras versiones tienen autenticación débil (basado en el valor de la comunidad) y no cifran la información, SNMP utiliza típicamente UDP como protocolo de transporte, los puertos UDP/161 y UDP/162 (traps) y aunque la última versión v3 cuenta con correctivos en la seguridad, no deja de ser vulnerable para una amenaza distribuida o de fuerza bruta con un diccionario potente.

Los dos factores determinantes para ejecutar el ataque son los siguientes:

En primer lugar, hay que recordar que en una comunicación basada en protocolo UDP (no orientada a la conexión) y por motivos de eficiencia, los datos se envían y se reciben sin verificar la conexión con el origen o destino, de la misma forma, se da por hecho la correcta entrega o recepción de datos.

En segundo lugar, el protocolo SNMP permite que se realicen consultas de gran volumen a través del tipo de solicitud llamado "GetBulkRequest", esta solicitud en la V2c se caracteriza por que el tamaño de su respuesta (423-1560 Bytes) es mucho más grande que el de la solicitud (0-102 Bytes), esto significa que existe un efecto de amplificación ya que la respuesta es más grande que la solicitud. (Security By Default, 2014)

De acuerdo a lo explicado, a todas las solicitudes SNMP tipo GetBulkRequest que se hagan a un servidor SNMP, el mismo dará respuestas de gran tamaño a IP la víctima, para ver su funcionamiento técnicamente se utilizara la herramienta snmp-DDOS para efectuar el ataque. (Security By Default, 2014)

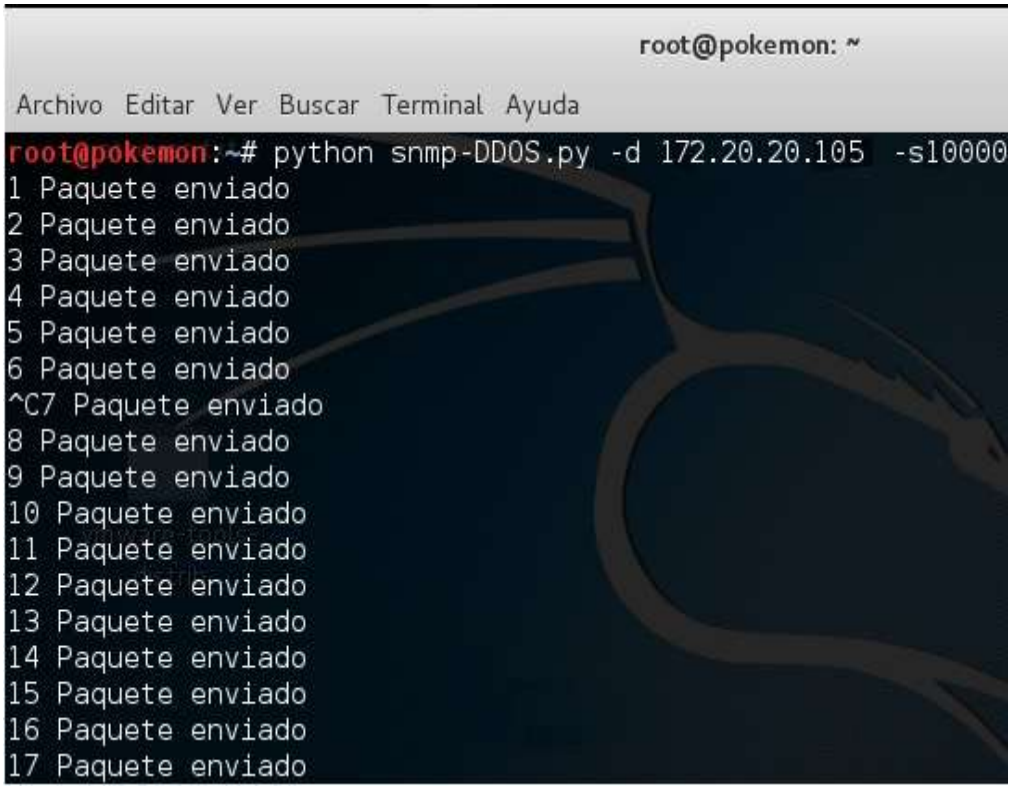


Figura 26-5: Herramienta snmp-DDoS realizando 1.000.000 ataques simultáneos
Realizado por: Fabián Hurtado, 2016

El ataque es realizado con mayor facilidad directamente al Firewall, ya que NMAP nos reportó que la dirección ip 172.20.20.105 (fw) mapea el protocolo SNMP hacia la Internet y la dirección ip interna 192.168.202.3, que en realidad no se debería conocer, sin embargo, esta ayuda fue brindada por medio del ataque de "fuerza bruta" realizado anteriormente donde una de las respuestas fue la dirección ip, puerto y protocolo utilizado:

Figura 27-5: Información del ataque de F. Bruta realizado
Realizado por: Fabián Hurtado, 2016

En la Figura 28-5, se muestra el progreso del ataque y como solo 1 PC de 1 atacante esta afectando el 25% del performance total del procesador de nuestro HONEYPOT-ROUTER, el ataque real como minimo deberia ser con 3 atacantes.

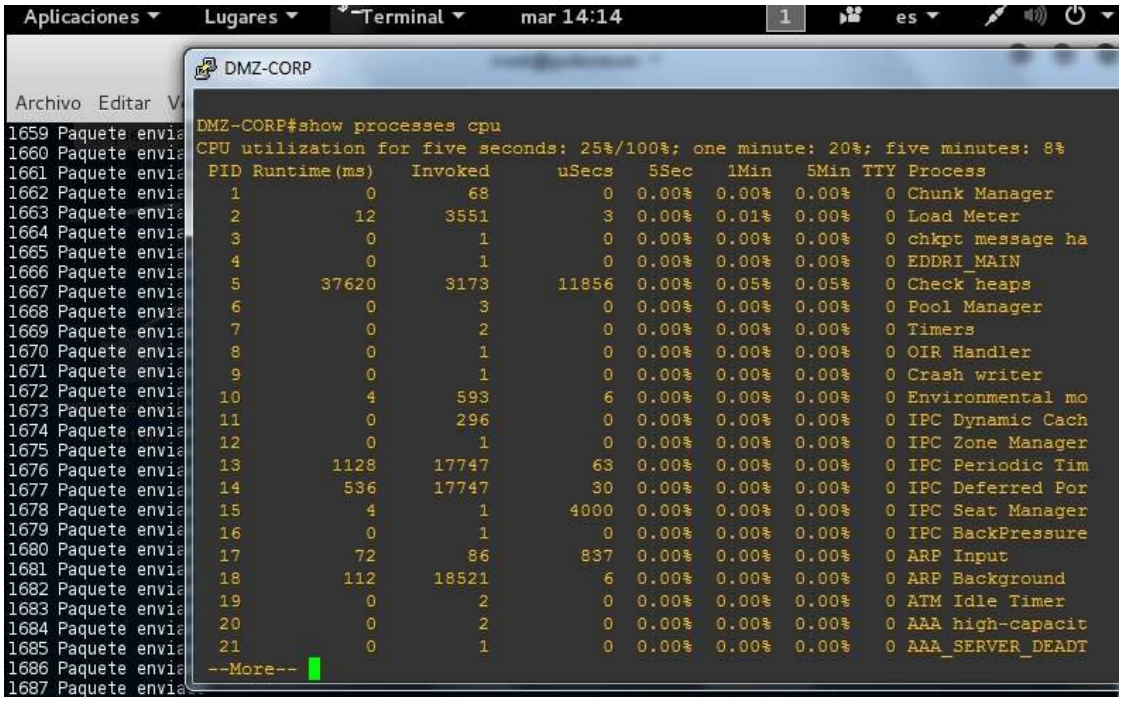


Figura 18-5: Desempeño del CPU con ataque DDoS - 1 solo PC
Realizado por: Fabián Hurtado, 2016

Ahora se visualizará el ataque realizado al Firewall el cual mapea el protocolo SNMP abierto desde el HONEYPOT-ROUTER. Se puede notar que el ataque realiza un getBulkRequest de 97 Bytes y la respuesta tiene un peso de 1459 Bytes, o sea, 15 veces más grande. Esto lo podemos observar con la herramienta OpenSource modo texto llamada T-Shark.

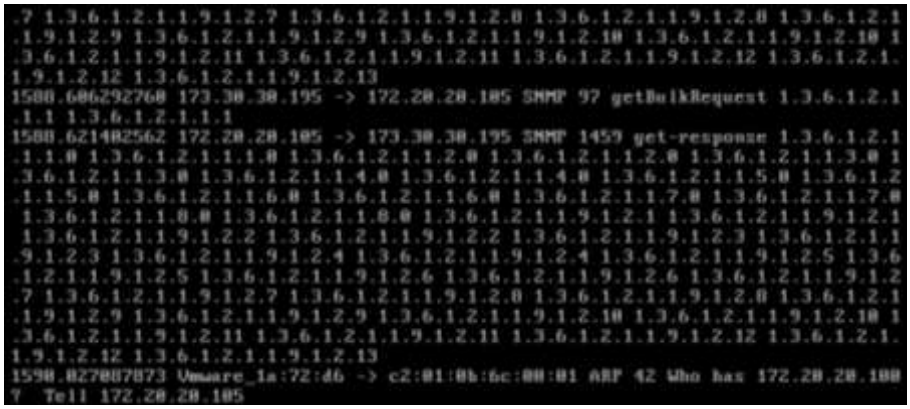


Figura 29-5: Ataque DDos en Firewall visto con TShark
Realizado por: Fabián Hurtado, 2016

Ahora se visualiza el ataque desde WIRESHARK.

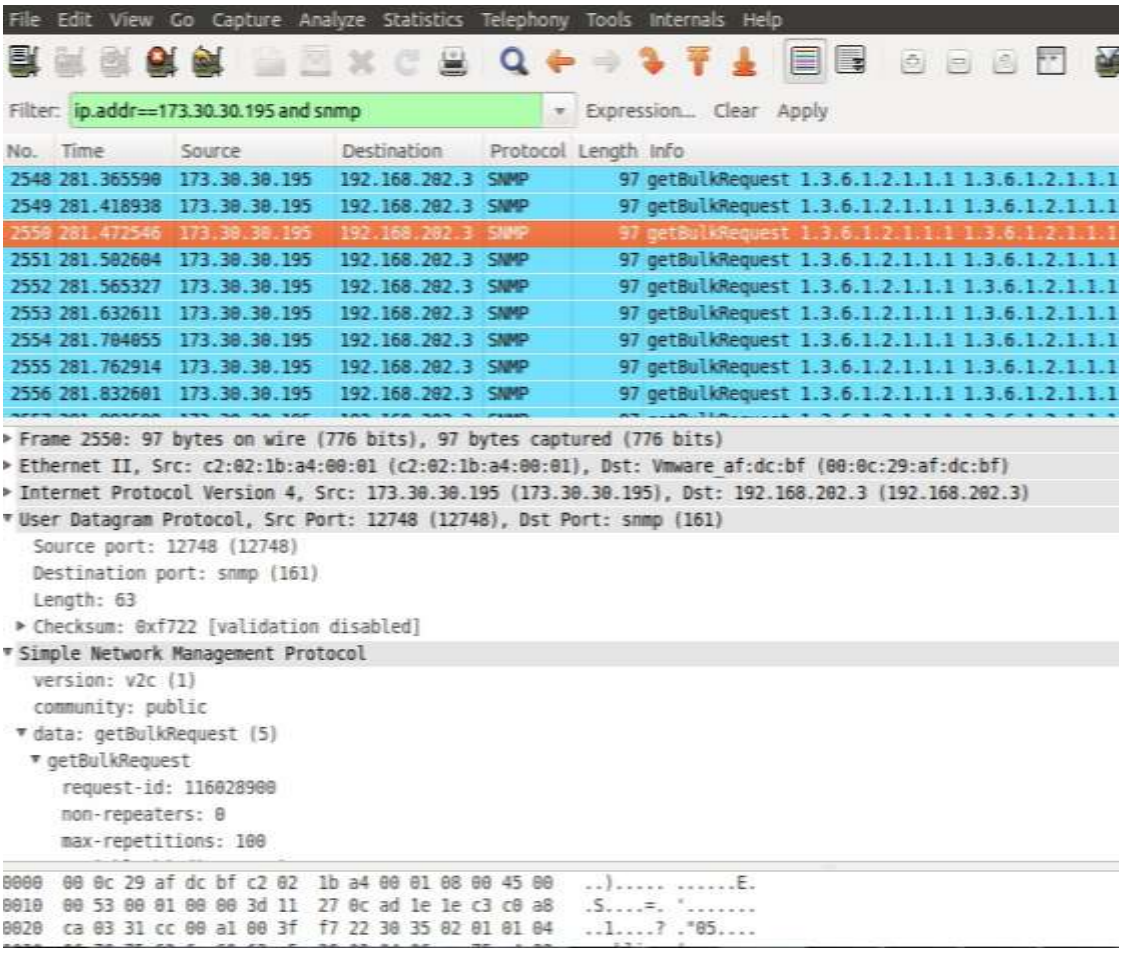


Figura 30-5. El mismo ataque visto con Wireshark desde 1 equipo interno
Realizado por: Fabián Hurtado, 2016

Como es un intento de extracción de información por la comunidad “public” y esta regla ya fue realizada para el ataque de fuerza bruta, así aparecerá en el SNORT/IDS.

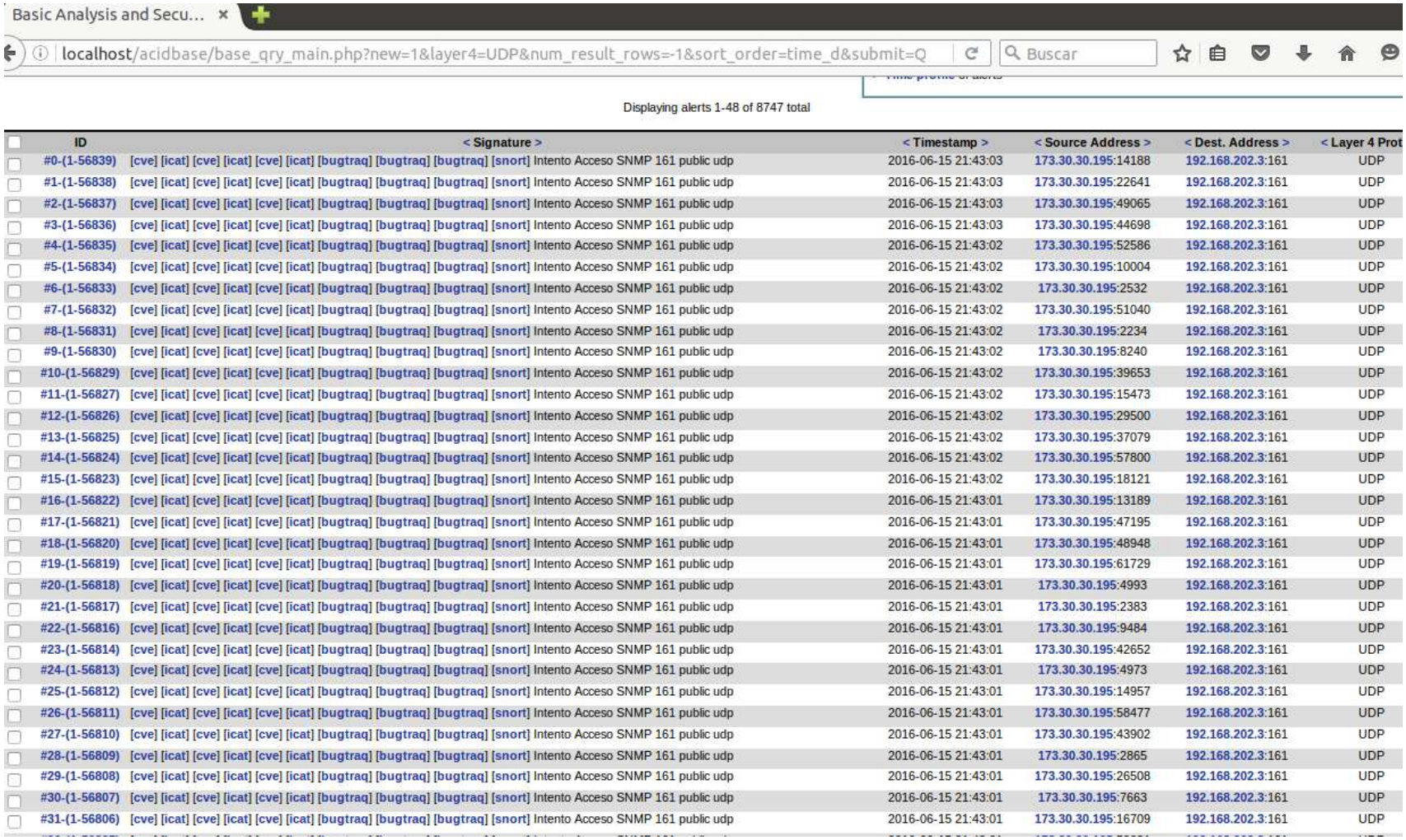


Figura 31-5: Ataque DDos - Visualizador de ataques ACIDBAE
Realizado por: Fabián Hurtado, 2016

Aquí se muestran una parte de las 2.041 entradas producto del ataque solo a la comunidad "public" ya que el programa snmp-DDOS está programado de tal forma que si no se ingresa el nombre de la comunidad, toma por DEFAULT el nombre de la comunidad "public", también se aprecia que el número de puerto, tampoco es ingresado por lo que el programa está diseñado para que si no se lo hace se toma por defecto el puerto 161 de tipo UDP, y por último se observa en dicha programación que el ataque toma por default que la versión del protocolo SNMP es la 2c, ya que es la más común para soportar getBulkRequest.

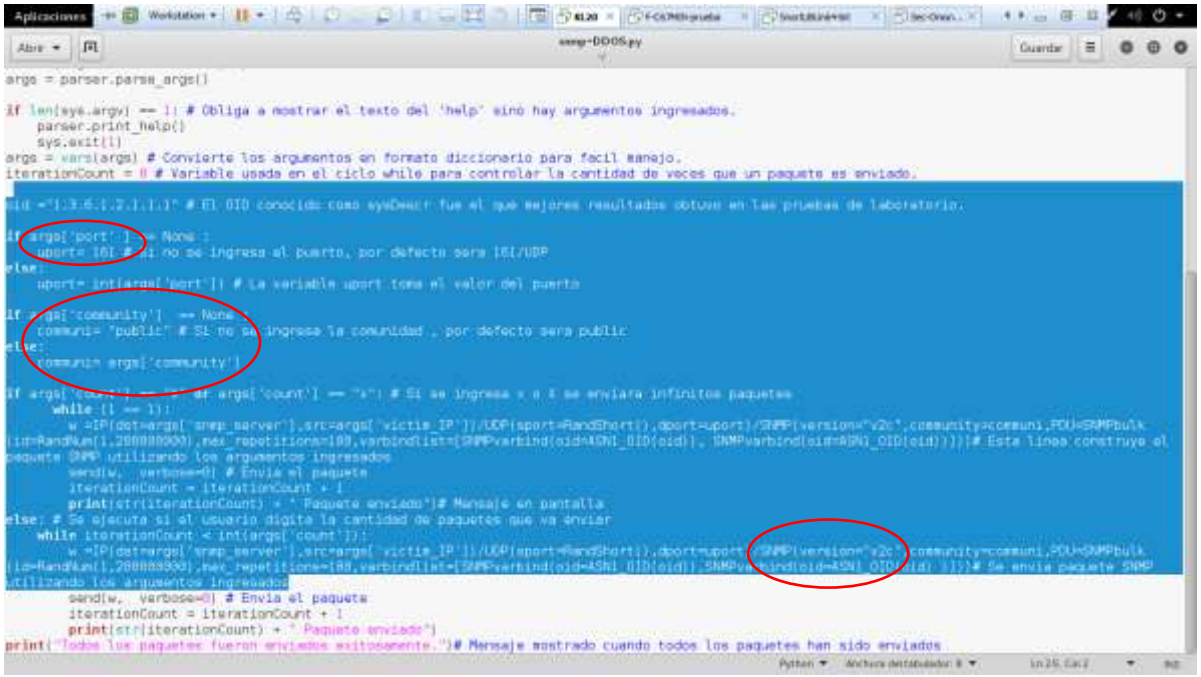


Figura 32-5: Código de programación snmp-DDOS.py
Realizado por: Fabián Hurtado, 2016

En cuanto al OID, se solicita información del 1.3.6.1.2.1.1.1 (descripción del sistema), el cual, según el creador de la aplicación, es el que mejores resultados ha dado realizando pruebas de laboratorio.(Exploting SNMP for DDoS «snmpddos», s. f.) Lo interesante de esto es que, el trabajo solo se lo realiza con 1 PC y el rendimiento del procesador del Router baja un 25%. En cuanto al consumo de memoria, se eleva un 27% (34000664 = 34 Mb)

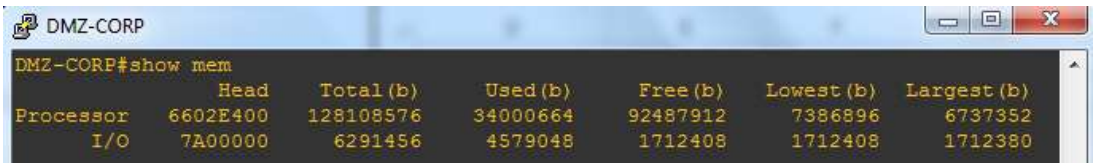


Figura 33-5: Desempeño de la memoria
Realizado por: Fabián Hurtado, 2016

Simples matemáticas. DDoS al ser distribuido, cuanto afectara al procesador del HONEYPOT-ROUTER, si el ataque es realizado de forma continua por 10, 20 o 30 atacantes?

A continuacion se presenta un resumen de los ataques realizados

Tabla 1-5: Ataques antes de solución

ATAQUES	UTILZ. CPU	UTILZ. MEM.
DDOS 3PC's	75,00%	80,00%
F.Bruta	18,00%	16,50%
Rastreo Ptos.	1,00%	5,20%

Realizado por: Fabián Hurtado, 2016

Ahora se procede a revisar todas las contramedidas para mitigar los ataques realizados.

Estas medidas se las da, tomando en cuenta que los ataques son muy letales, desde el que tiene un RIESGO BAJO, hasta el que tiene el RIESGO ALTO, ya que al efectuarlo, desborda la capacidad de procesamiento del HONEYPOT-ROUTER y no permite el correcto funcionamiento del mismo.

En primer lugar, se propone una infraestructura de solución a la que se la denominará SEGURA, ya que luego de estudiar cada uno de las amenazas al protocolo SNMP se pretende bloquearlas, brindando y mejorando el performance de tanto en procesamiento y memoria del Router de Frontera que atrae a los atacantes.

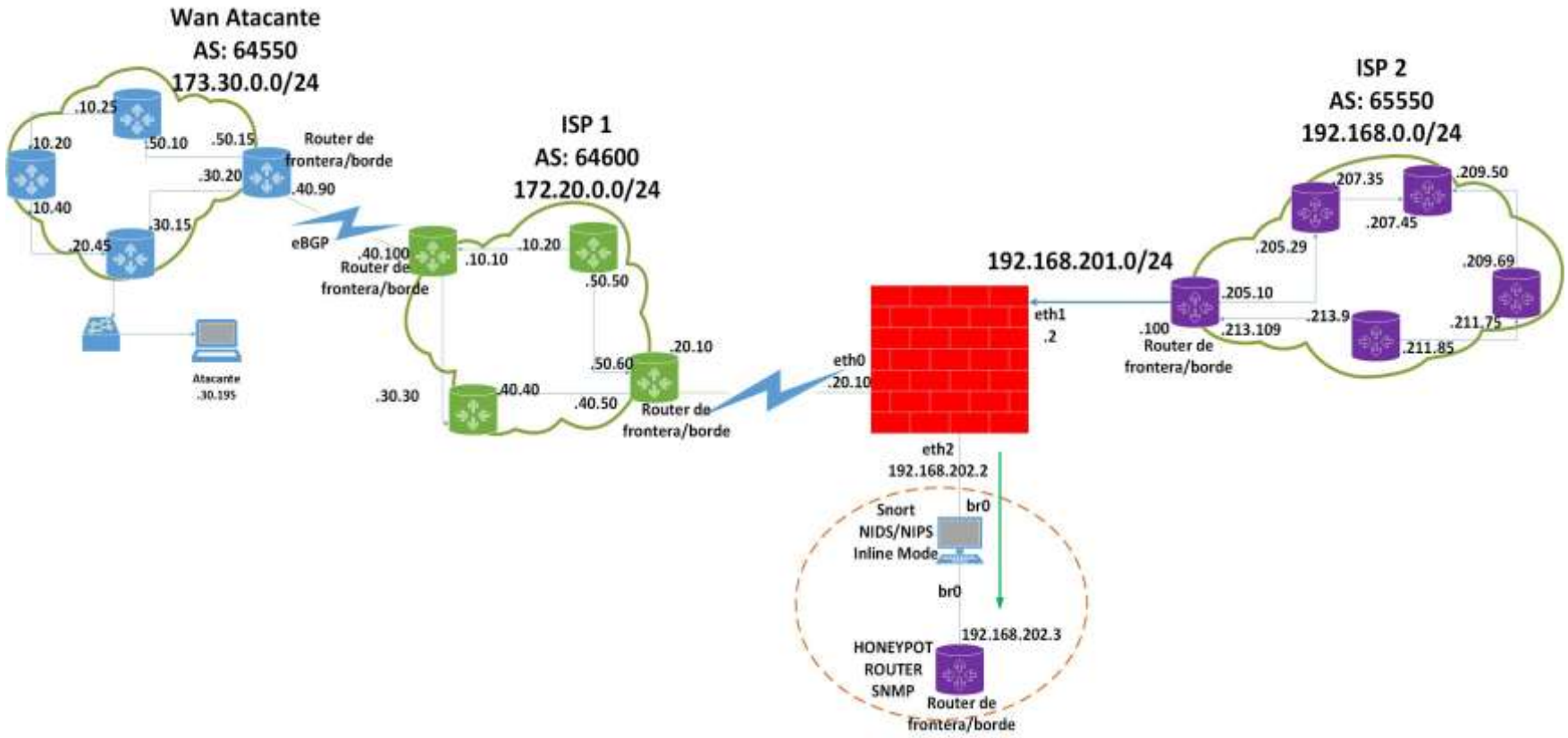


Figura 34-5: Infraestructura de solución propuesta como contramedida para mitigar los ataques realizados
Realizado por: Fabián Hurtado, 2016

Revisando y estudiando los resultados de las pruebas realizadas a las diferentes amenazas, los ataques tenían un común denominador, el tiempo en el cual se efectuaron cada uno, por lo que se investigó a fondo, si existía alguna forma de mitigar ataques realizados en periodos excesivamente cortos. No es normal que las solicitudes de GETBULK se realicen, como en el caso de DDOS, demasiadas y en un periodo muy corto (hablando de segundos) de tiempo, por este motivo, a este tipo de paquetes son considerados "ingreso o petición no adecuada".

Eventos Filter

Los eventos "filter" son una forma alterna de bloquear alertas en un IPS tomando muy en cuenta su SID (Signature ID). Rate_filter, una variante en las sentencias "filter" provee un bloqueo (en caso de ser esa la acción a tomar) basado en el tiempo en que el evento alert este activado o comience activarse.(Snort, 2011)

Luego de realizar un ataque con NMAP hacia la infraestructura HONEYPOT-ROUTER, ya teniendo la infraestructura "Filter" en marcha con la acción a tomar DROP (Bloqueo Paquetes) tenemos el siguiente resultado.

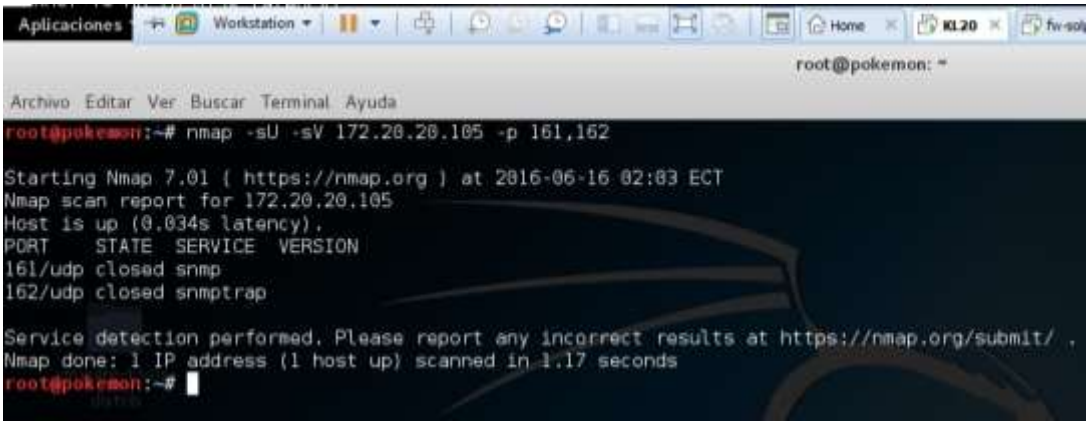


Figura 35-5: Ataque Rastreo de Puertos detectado y bloqueado por Snort NIDS/NIPS
Realizado por: Fabián Hurtado, 2016

El ataque se repele/bloquea paquetes denominados "ingreso o petición no adecuada" de la siguiente manera, al final del archivo /etc/snort/snort.conf.

```
#Corto a peticion en puerto 161 Y 162 - NMAP
rate_filter gen_id 1, sig_id 1417, track by_src, count 1, seconds 1, new_action drop, timeout 1
rate_filter gen_id 1, sig_id 1419, track by_src, count 1, seconds 1, new_action drop, timeout 1
```

Figura 36-5: Configuración de firma (regla) detecta y bloquea en archivo /etc/snort/snort.conf

Realizado por: Fabián Hurtado, 2016

En la sentencia claramente se toma la acción DROP a la Alerta con Sig_ID 1417 y 1419, las cuales nos alertan sobre entradas específicas en los puertos 161 y 162.

Para ejecutar el Snort/NIPS o modo INLINE se utiliza la sentencia:

snort -Q --daq nfq --daq-mode inline --daq-var queue=0 -c /etc/snort/snort.conf -A Console

-Q= habilita el modo INLINE, --daq nfq: habilitada la adquisición de paquetes, --daq-mode inline: selecciona el modo INLINE, --daq-var queue=0: se habilita la cola por donde van a ingresar los ataques COLA 0, -c: indica el archivo de reglas a ejecutar, -A Console: mostrar resultados por consola

Luego se habilita la Cola 0 con el siguiente comando:

iptables -I FORWARD -j NFQUEUE --queue-num 0

Esta imagen muestra el bloqueo realizado

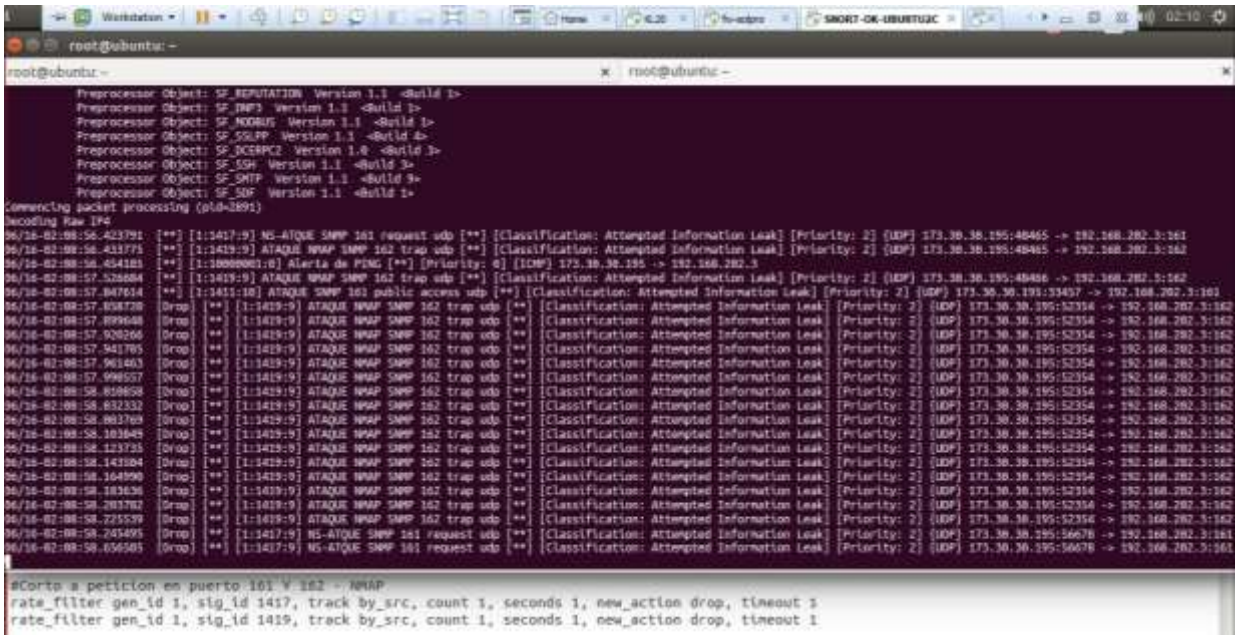


Figura 37-5. Mensajes DROP (bloqueo) de paquetes detectados

Realizado por: Fabián Hurtado, 2016

Mensajes Drop – Bloqueos de ataques realizados.

Figura 38-5: Mensajes DROP ampliados
Realizado por: Fabián Hurtado, 2016

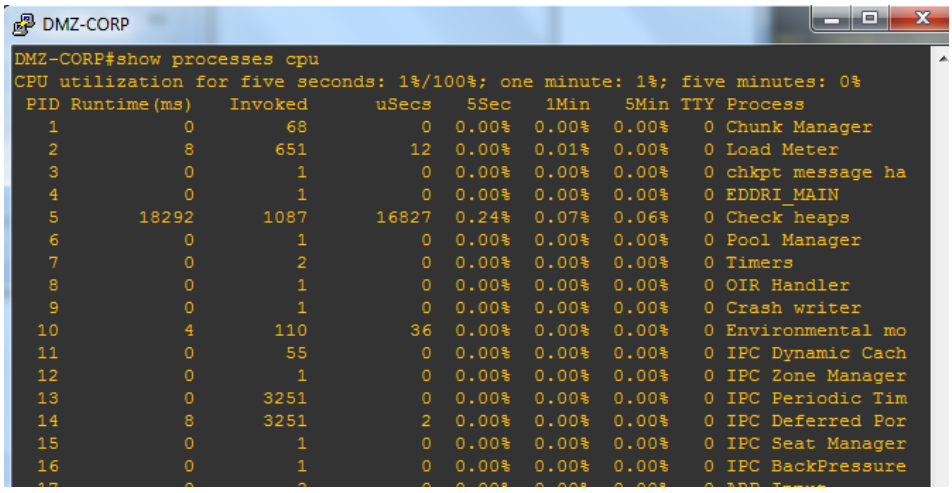


Figura 39-5: Desempeño de CPU del Router atacado
Realizado por: Fabián Hurtado, 2016

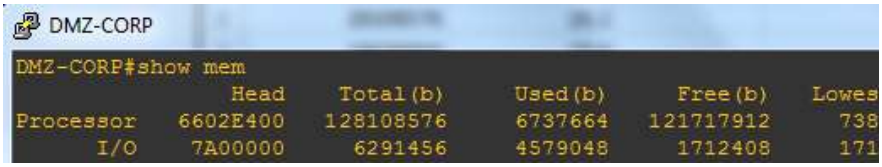


Figura 20-5: Desempeño de la memoria del Router atacado
Realizado por: Fabián Hurtado, 2016

Claramente se observa que no hay afectación en el consumo de recursos en el HONEYPOT-ROUTER, CPU (1%) y memoria 5,23% (6,73Mb), lo mínimo para poder trabajar.

El ataque que sigue en el orden tomando en cuenta el Riesgo Mediano es, la amenaza de Fuerza Bruta o Ataque de Diccionario, el cual también entra en los que utilizan tiempos cortos.

Realizando el ataque, habiendo ya configurada la sentencia RATE_FILTER, el resultado que nos entrega la propia herramienta de snmp-brute es fenomenal, ya que luego de ejecutar el

ataque, el mensaje que aparece indica **No Community string found,** en otras palabras, "*los nombres de comunidades no fueron encontrados*".

Aquí la imagen del frustrado ataque en la máquina del pirata informático y el resultado en el Snort/NIDS/NIPS.

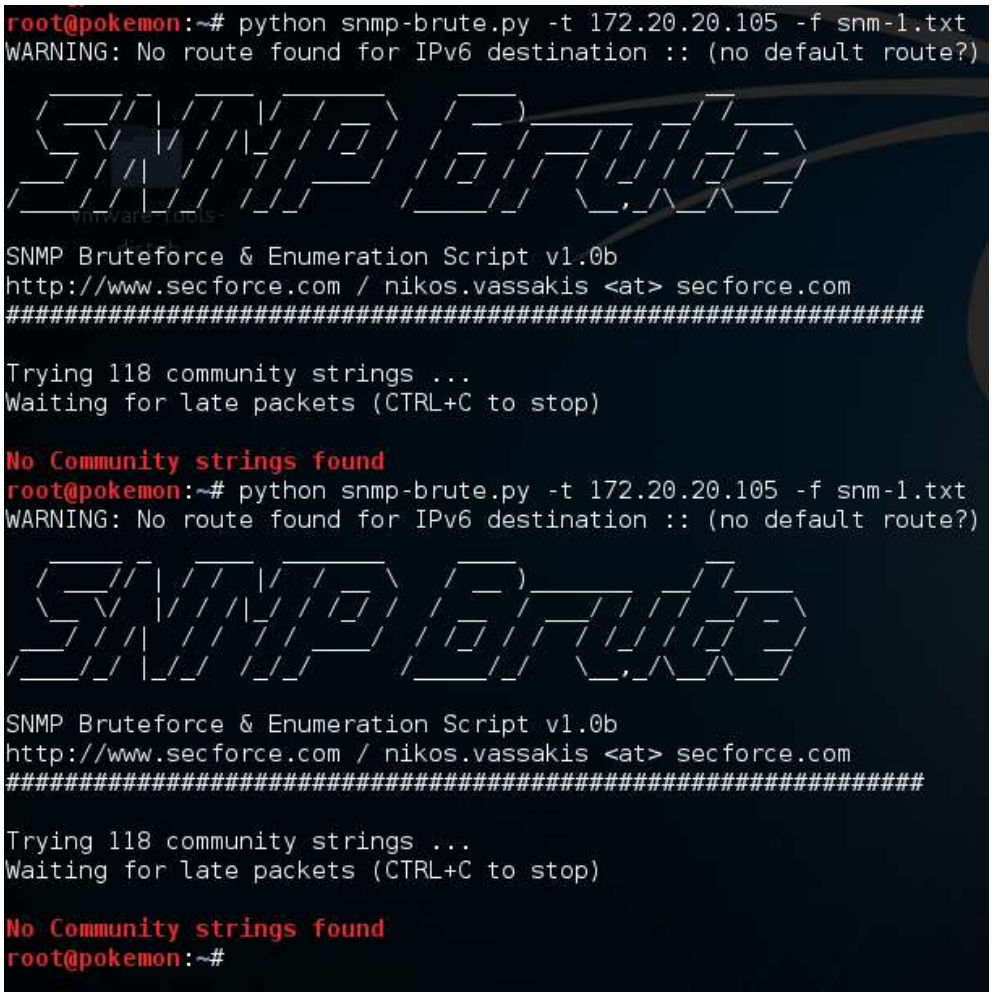


Figura 41-5. Ataques de Fuerza Bruta / Diccionario fallidos
Realizado por: Fabián Hurtado, 2016

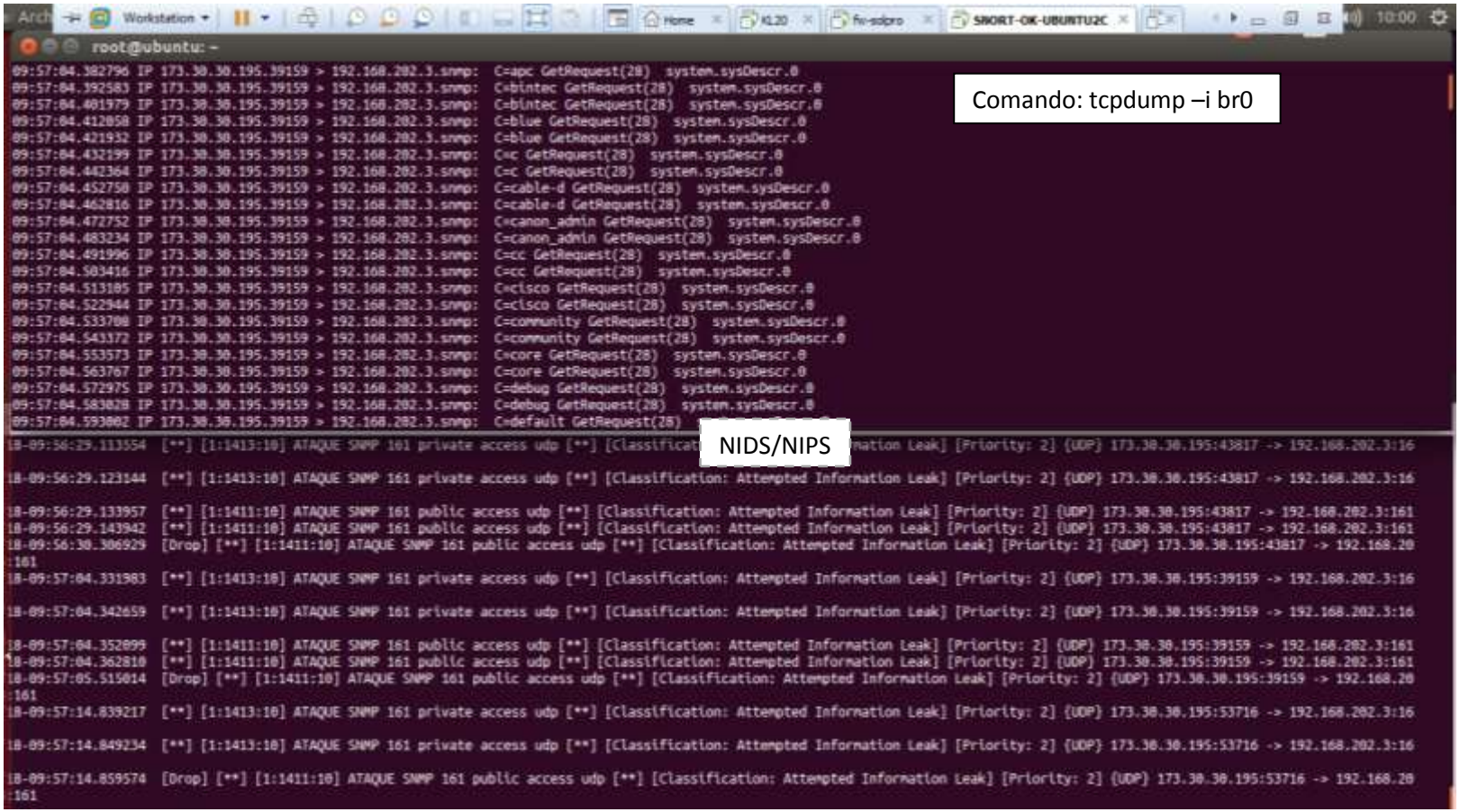


Figura 42-5: Mensajes DROP (bloqueo) de ataque F.B. Diccionario
Realizado por: Fabián Hurtado, 2016

Aquí se muestran las entradas por la interfaz en modo bridge "br0" con el comando TCPDUMP y el bloqueo del ataque vía consola con:

snort -Q --daq nfq --daq-mode inline --daq-var queue=0 -c /etc/snort/snort.conf -A Console

Previo a esto se habilitó la Cola 0 con el siguiente comando:

iptables -I FORWARD -j NFQUEUE --queue-num 0

La sentencia de bloqueo es la siguiente:

#Intento de extracción de información por la comunidad Public y Private

#Corto a la 3era petición en puerto 161 (public)

rate_filter gen_id 1, sig_id 1411, track by_src, count 2, seconds 5, new_action drop, timeout 15

#Corto a la 3era petición en puerto 161 (private)

rate_filter gen_id 1, sig_id 1413, track by_src, count 2, seconds 5, new_action drop, timeout 15

Las 2 sentencias tienen como objetivo la acción DROP en el Signature ID # 1411 y 1413, los cuales después de 2 entradas en menos de 5 segundos activan el bloqueo, aquí se visualiza la actividad en el HONEYPOT-ROUTER, como se tiene:

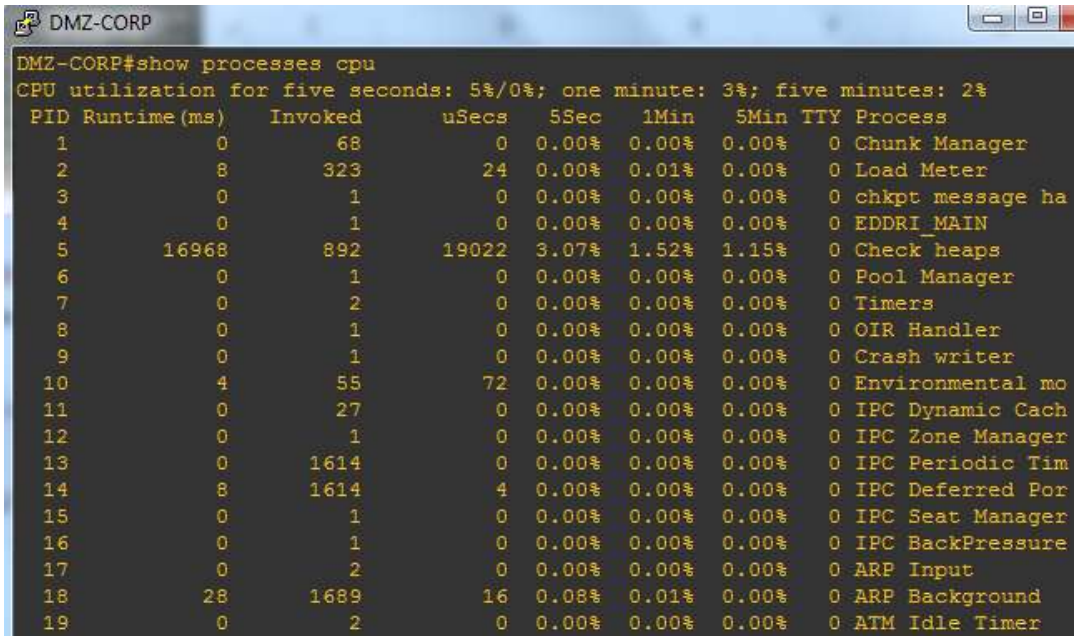


Figura 43-5: Desempeño del CPU-Router en pleno ataque FB-Dicc.
Realizado por: Fabián Hurtado, 2016

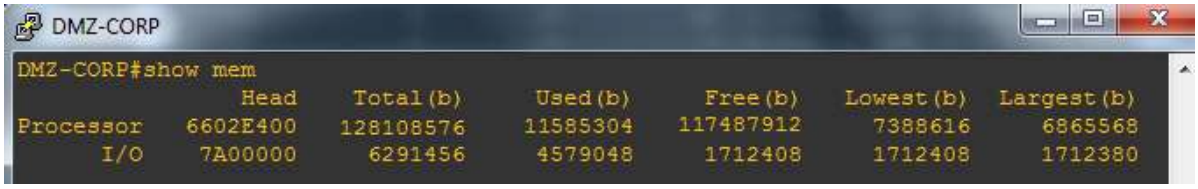


Figura 44-5: Desempeño de la Memoria-Router en pleno ataque FB-Dicc
Realizado por: Fabián Hurtado, 2016

Según la imagen, muestra que no hay afectación en el consumo de recursos del HONEYPOT-ROUTER, CPU (5%) y memoria 8,98% (11,58Mb), lo que indica que el bloqueo a la amenaza si dio sus frutos.

El ataque DDOS (Distributed Denial-of.Service) es muy letal ya que se ejecuta desde muchos maquinas al mismo tiempo, al ser este un procedimiento en volumen, es lo que lo hace eficaz. Por su rapidez es detectado a tiempo por la misma sentencia DROP de la amenaza tipo Fuerza Bruta:

#Corto a la 3era petición en puerto 161 (public)

rate_filter gen_id 1, sig_id 1411, track by_src, count 2, seconds 5, new_action drop, timeout 15.

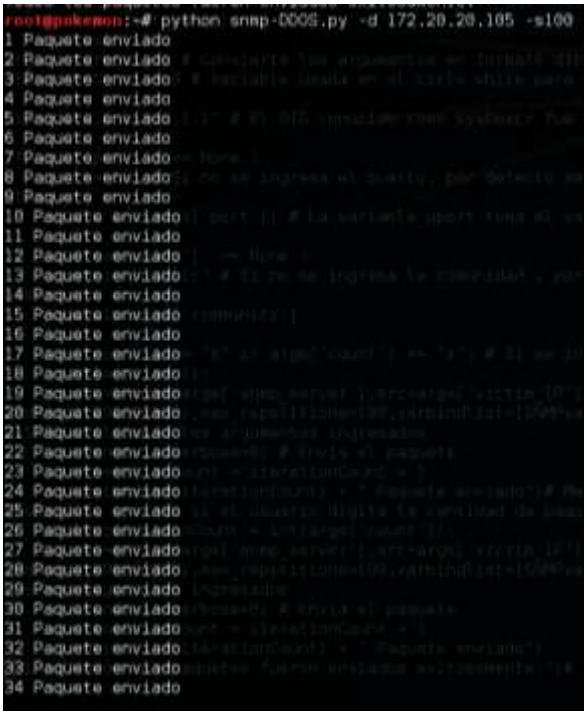


Figura 45-5: Ataque DDoS fallido
Realizado por: Fabián Hurtado, 2016

Como se puede visualizar, los paquetes maliciosos salen del ataque, pero al encontrarse con el Snort/NIPS son bloqueados oportunamente antes que causen problema a la infraestructura protegida, o sea, el HONEYPOT-ROUTER.

Aunque al final del ataque se vea en mensaje: ”Todos los paquetes fueron enviados exitosamente” (por que asi esta en la programacion del la herramienta) no causaron ningun efecto malicioso.

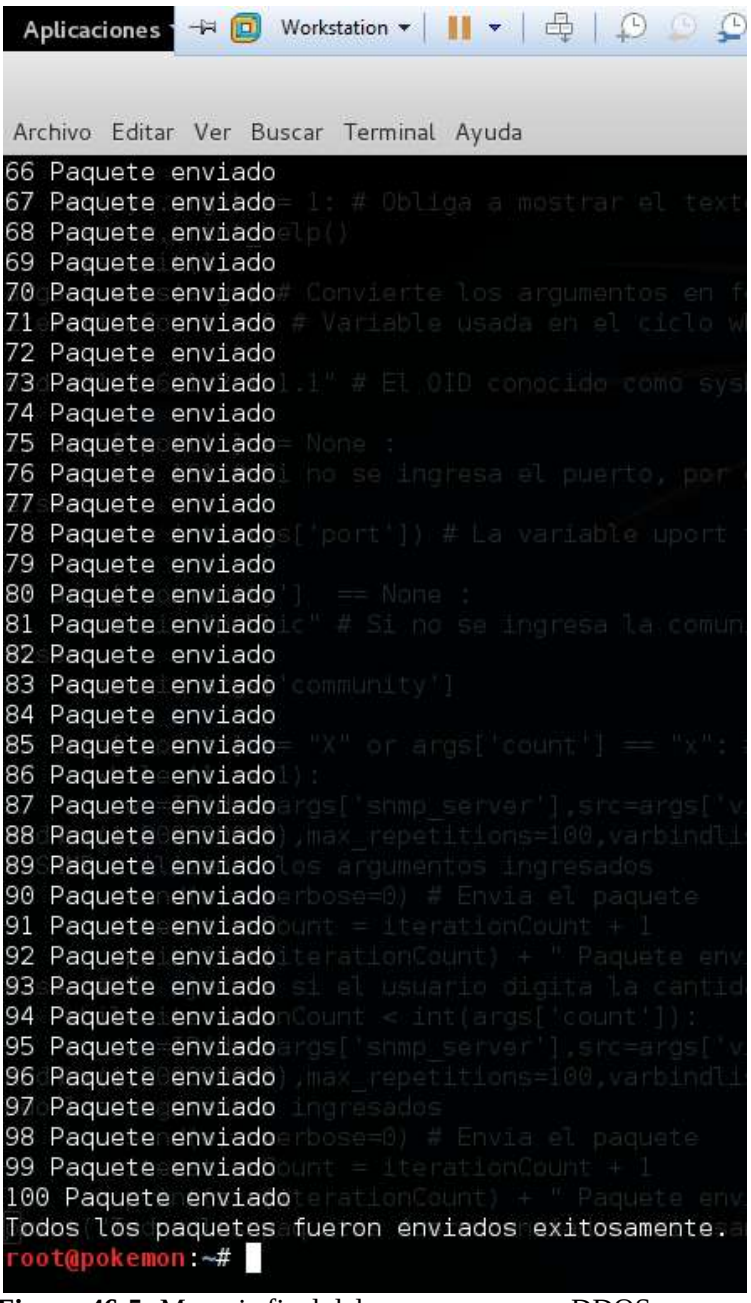


Figura 46-5: Mensaje final del programa snmp-DDOS .py
Realizado por: Fabián Hurtado, 2016

El consumo del procesador de la CPU de nuestro HONEYPOT-ROUTER es del 1%, como lo muestra la siguiente Figura.

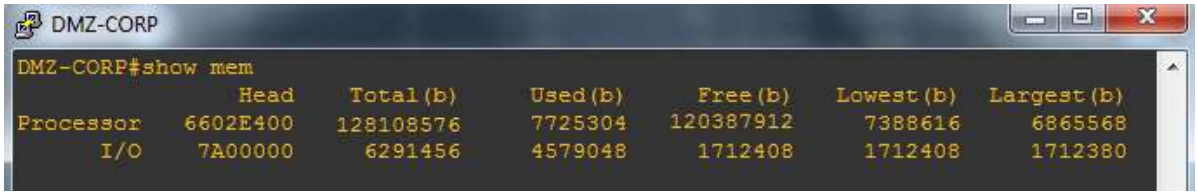


Figura 473-5: Desempeño de la Memoria-Router en pleno ataque DDoS
Realizado por: Fabián Hurtado, 2016

Tabla 2-5: Ataques después de la solución

ATAQUES	UTILZ. CPU	UTILZ. MEM.
DDoS x 3 PC's	3,00%	18,09%
F.Bruta	5,00%	8,98%
Rastreo Puertos	1,00%	5,23%

Realizado por: Fabián Hurtado, 2016

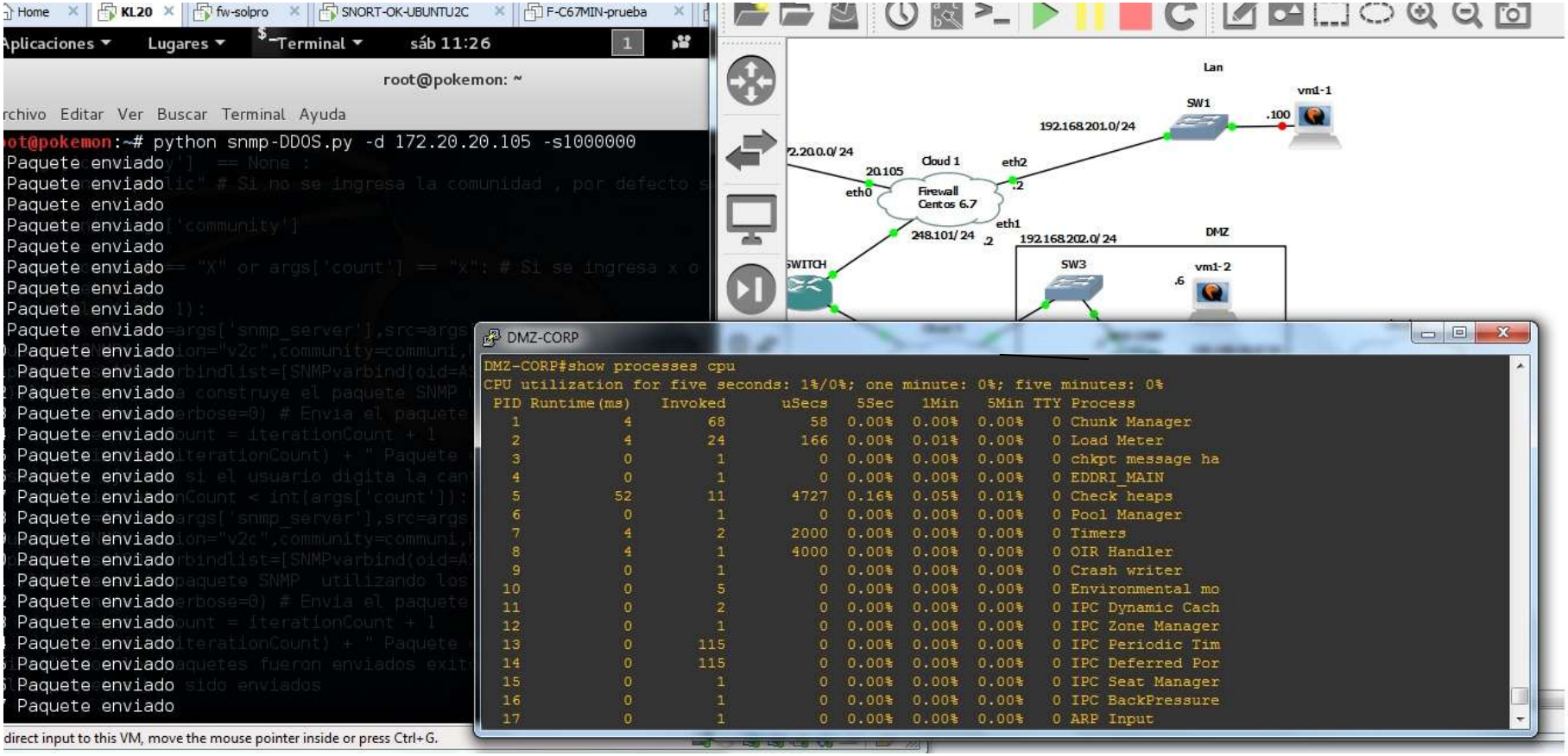


Figura 48-5. Desempeño del CPU-Router en pleno ataque DDoS
Realizado por: Fabián Hurtado, 2016

Las imágenes muestran que debido al bloqueo del ataque por medio del NIPS, no existe mayor consumo de recursos en el HONEYPOT-ROUTER, CPU (1%) y memoria 7,7 Mb (6.03%).

En segundo lugar y adicional a las infraestructuras de solución propuestas, se enumera una lista de mecanismos de seguridad con los cuales se pueden mitigar o prevenir amenazas y riesgos generados hacia nuestro Router de Frontera:

1. Actualizar el IOS, ya que la empresa Cisco en cada versión nueva que lanza al mercado incrementa la lista de versiones y variantes de ataques, también mejora y robustece a los procesos de detección de ataques más frecuentes. Hay que señalar que los equipos Cisco, dependiendo al sector que son requeridos o vendidos, cuentan con su propio performance o robustez, por lo consiguiente, tienen diferentes Sistemas Operativos como: IOS, IOS XE, IOS XR, NX-OS. (Cisco Systems, 2015)
2. Monitoreo constante del rendimiento de la memoria y procesador donde este activado el protocolo, ya que podría darse el caso que, aunque este mitigando las amenazas, el performance del equipo varíe por alguna otra razón, en el caso que sea Cisco, se lo realiza con los comandos show mem y show process cpu.
3. Monitoreo del throughput (ancho de banda consumido) de los enlaces en las interfaces del equipo que tenga activo el protocolo SNMP, para garantizar el ancho de banda en tiempo real de las interfaces o subinterface que se desee.
4. Actualización a la última versión de Snort IDS/IPS, las cuales traen sus respectivos parches de seguridad con lo cual se eleva el desempeño del sistema core. (https://snort.org/downloads)
5. Actualización de las últimas firmas disponibles de IDS e IPS, ya que al ser una comunidad FREE están en constante desarrollo y frecen muchas mejoras para nuevos tipos de amenazas, como APTs y de día cero. (https://snort.org/downloads)
6. Implementar una solución de Administración de Correlación de Eventos después del IPS donde se emitirán alertas, las cuales deberán ser revisadas por el ente de seguridad (Oficial de Seguridades). Al ser este tipo de Router un dispositivo de Borde o Frontera, estará expuesto a cientos de miles eventos/amenazas por el ato tráfico que maneja (por estar al borde el internet). Por tal motivo, no se pondría a un ser humano a revisar línea por línea y que correlacione el evento para identificar su tipo. Un buen ejemplo de este tipo de software es Alienvault OSSIM.
7. NO utilizar configuraciones por defecto en el software y hardware que se adquiera, sobre todo porque no traen endurecimiento o cambios personalizados, los cuales sirven para ayudar a la seguridad y al correcto funcionamiento del entorno al cual son instalados.

CONCLUSIONES

- Para el escenario de red propuesto basado en el estudio de los resultados de una honeypot virtual de los riesgos generados por amenazas en routers de frontera se utilizaron herramientas de análisis de trafico como Tshark y Wireskark, herramientas de escaneo y ataques ya direccionadas hacia el protocolo SNMP como Kali Linux, Nmap, SNMP-Brute.py, snmp-DDOS.py, donde fue posible identificar sus vulnerabilidades; permitiendo la ejecución de ataques Visualización de información / rastreo de puertos, Denegación de servicio distribuido y Fuerza bruta / diccionario, con mayor impacto en la disponibilidad y confiabilidad de la información.

- Se desarrolló una solución llamada HONEYPOT ROUTER SNMP, que contiene 2 etapas: a) Estudio y detección de vulnerabilidades y ataques, b) Aplicar la protección y medidas de seguridad; considerando las recomendaciones de seguridad de los estándares y normas internacionales ISO/IEC 27001, NIST y mejores prácticas de CISCO, así como también recomendaciones y técnicas de reconocimiento del Libro HONEYPOTS Traking hackers (Lance Spitzner) y el Paper Honeypot Router for routing protocols protection (Abdallah Ghourabi, Tarek Abbes y Adel Bouhoula) que permiten tener una idea clara y una referencia de trabajo estándar que facilita las tareas de elaboración del presente trabajo de investigación.

- Mediante la implementación de la solución propuesta HONEYPOT ROUTER SNMP, en un ambiente de red simulado se logró minimizar en un 95% las vulnerabilidades y amenazas en relación al mismo escenario sin mecanismo de seguridad. Al reducir notablemente los riegos se consiguió mejorar el performance, rendimiento del CPU y rendimiento de la memoria en los routers de frontera, garantizando así la continuidad del negocio.

- Con el empleo de la estadística inferencial chi-cuadrado y un nivel de significancia de 0.05, de acuerdo a la tabla de distribución se obtiene que X2 Tabla 12.592 y el valor calculado X2 Calculado en esta investigación es de 15.292, notando que es superior al valor de la tabla de distribución, por lo que el valor de X2calculado se encuentra en el sector de NO Aceptación de Ho y resulta estadísticamente significativa, Aceptando la hipótesis de investigación Hi.

- Finalmente se proponen 7 puntos esenciales para la mitigación de amenazas y riesgos y una infraestructura llamada Honeypot Router y la cual ofrece un entorno robusto y confiable ya que no solo se detectan vulnerabilidades, sino que también se previenen/bloquean.

RECOMENDACIONES

- No se recomienda utilizar las configuraciones que vienen por default en los Routers o cualquier equipo, ya que como se demostró y todo caso es diferente, este tipo de seteos viene con vulnerabilidades abiertas/disponibles por lo que los atacantes saben exactamente por donde atacar.

- De acuerdo a los resultados obtenidos en este estudio, podemos determinar que la seguridad no depende de un solo factor de riesgo, sino de varios, por lo que no se recomienda utilizar el Firewall como único dispositivo de seguridad.

- En el caso del Firewall, se recomienda configurar políticas de acceso, para realizar un filtro exclusivamente del trafico SNMP a direcciones IP Publicas específicas.

- Se recomienda tener más de un punto de visualización para poder determinar eventos como amenazas, ataques etc. Estos puntos de visualización deben ser administrados por un Oficial de Seguridad de la Información.

- De acuerdo al estudio de esta investigación se recomienda crear de mejor manera, una Infraestructura de Red con un alto grado de seguridad conformada por software y hardware como: VLan, UTMs, Firewalls, IDS, IPS, equipos anti IP Spoofing.

- Se recomienda el uso de servicios pagados que actualmente existen en la nube para prevenir ataques DDoS, o software freeware que cumplen con la misma función, solo que en menor escala.

BIBLIOGRAFIA

[1]. **CHANG, H., WU, S., JOU, Y**. (2010). Real-time protocol analysis for detecting link-state routing protocol attacks. *ACM Transactions on Information and System Security (TISSEC)*. https://doi.org/10.1145/383775.383776

[2]. **CISCO SYSTEMS.** (2004). Extensions to BGP to Support Secure Origin BGP (so BGP). Recuperado a partir de https://tools.ietf.org/html/draft-ng-sobgp-bgp-extensions-02

[3]. **CISCO SYSTEMS.** (2006, marzo). Exploring Autonomous System Numbers - Ccnp Routing. Recuperado a partir de http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-12/autonomous-system-numbers.html

[4]. **CISCO SYSTEMS.** (2010a, Diciembre). Distributed Denial of Service Attacks - The Internet Protocol Journal - Volume 7, Number 4. Recuperado a partir de http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html

[5]. **CISCO SYSTEMS.** (2010b). Switching y routing CCNA: Principios básicos de routing y switching. Recuperado a partir de https://es.scribd.com/doc/265458388/ccna-2-word-resuelt-pdf

[6]. **CISCO SYSTEMS.** (2015, febrero). Networking Software (IOS & NX-OS). Recuperado a partir de http://www.cisco.com/c/en/us/products/ios-nx-os-software/index.html

[7]. **CISCO SYSTEMS.** (2016a). Border Gateway Protocol (BGP). Recuperado a partir de http://www.cisco.com/c/en/us/products/ios-nx-os-software/border-gateway-protocol-bgp/index.html

[8]. **CISCO SYSTEMS.** (2016b, febrero). Cisco Advanced Routing. Recuperado a partir de http://www.cisco.com/networkers/nw00/pres/2200.pdf

[9]. **CISCO SYSTEMS.** (2016c, junio). Cisco ASR 9922 Router. Recuperado a partir de http://www.cisco.com/c/en/us/products/routers/asr-9922-router/index.html

[10]. **CISCO SYSTEMS.** (2016d, noviembre). Tendencia de amenazas al protocol SNMP. Recuperado a partir de http://www.cisco.com/c/en/us/products/security/security-reports.html

[11]. **CRESPATA, R.** (2012, marzo). *Análisis del protocolo SNMPv3 para el desarrollo de un prototipo de monitoreo de red segura*. Escuela Superior Politécnica del Chimborazo, Riobamba.

[12]. **EVANGELOS KRANAKIS, T. W**. (2010). Pretty Secure BGP (psBGP). *IEEE*. Recuperado a partir de http://people.scs.carleton.ca/~kranakis/Papers/TR-04-07.pdf

[13]. **GEORGE CYBENKO. (**2012, febrero). Multiple Vulnerabilities in SNMP. Recuperado a partir de http://www.ists.dartmouth.edu/library/9.pdf

[14]. **GEROMETA, O**. (2011). Apunte Rápido CCENT versión 5.0. Recuperado a partir de https://es.scribd.com/document/336467249/Apunte-Rapido-CCENT-version-5-0

[15]. **GHOURABI, A., ABBES, T., BOUHOULA, A.** (2010). Honeypot router for routing protocols protection. https://doi.org/10.1109/CRISIS.2009.5411968

[16]. **HANDLEY, M. J., & RESCORLA, E.** (2006, noviembre). Internet Denial-of-Service Considerations. *The IETF Trust*.

[17]. **HONAN, B.** (2010). *ISO/IEC 27001 Security & Governance*. It Governance Ltd. Recuperado a partir de http://dl.acm.org/citation.cfm?id=1855249

[18]. **HU, Y., PERRIG, A., JOHNSON, D**. (2006). Efficient Security Mechanisms for Routing Protocols.

[19]. **HUAWEI.** (2015, febrero). NetEngine5000E Cluster Routers. Recuperado a partir de http://e.huawei.com/en/products/enterprise-networking/routers/ne/ne5000e

[20]. **JUNIPER.COM.** (2015, junio). MX2020 Physical Specifications - Technical Documentation Support - Juniper Networks. Recuperado a partir de http://www.juniper.net/documentation/en_US/release-independent/junos/topics/reference/specifications/mx2020-physical.html

[21]. **KENT, S., LYNN, C., & SEO, K**. (2010, Abril). Secure Border Gateway Protocol (S-BGP). IEEE. Recuperado a partir de http://ieeexplore.ieee.org/document/839934/

[22]. **LARIOS, A., MOREIRA, B.** (2011, julio). *Border Router Cisco - CCNP ROUTING*. Universidad Nacional Autónoma de Nicaragua-León, Leon, Nicaragua. Recuperado a partir de http://riul.unanleon.edu.ni:8080/jspui/bitstream/123456789/2476/1/208271.pdf

[23]. **LINUCA**. (2008, Agosto). SNORT+MYSQL+ACID: Sistema de detección de intrusos open source. Recuperado a partir de http://beta.redes-linux.com/manuales/seguridad/snort_Mysql_acid.pdf

[24]. **MITTAL,V. & VIGNA, G**. (2008, noviembre). Sensor-based intrusion detection for intra-domain distance-vector routing. Recuperado a partir de http://dl.acm.org/citation.cfm?id=586129

[25]. MURPHY, S. L., & BADGER, M. R. (2006). Digital signature protection of the OSPF routing protocol. IEE**E.**

[26]. **NICHOLAS MARCH.** (2010). *Nmap Cookbook*. Recuperado a partir de https://docs.google.com/file/d/0B6Vlr2bSsrysdHFqWklySXBFYUU/view

[27]. **NIST NATIONAL INSTITUTE OF STANDAR AND TECHNOLOGY.** (2007, julio). NIST 800-54 Border Gateway Protocol Security. Recuperado a partir de http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-54.pdf

[28]. **NIST NATIONAL INSTITUTE OF STANDAR AND TECHNOLOGY.** (2015, mayo). NIST 800-82 Guide to Industrial Control Systems (ICS) Security. Recuperado a partir de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[29]. **NMAP.** (2012, Enero). Snmp-brute NSE Script. Recuperado a partir de https://nmap.org/nsedoc/scripts/snmp-brute.htm

[30]. **NMAP.** (2016a, Enero). Nmap Change Log. Recuperado a partir de https://nmap.org/changelog.html

[31]. **NMAP.** (2016b, junio). Nmap: the Network Mapper - Free Security Scanner. Recuperado a partir de https://nmap.org/

[32]. **OULU, U. (**2010, Enero). PROTOS: Security testing of protcol implementations. Recuperado a partir de https://www.ee.oulu.fi/roles/ouspg/

[33]. **PAZMIÑO, L.** (2011, noviembre). *Análisis de la tecnología Honeypot y su aplicación en la detección y corrección de vulnerabilidades en la red de datos del gobierno autónomo descentralizado de la provincia del Chimborazo*. Escuela Superior Politécnica del Chimborazo, Riobamba.

[34]. **PORTAL DE ADMINISTRACIÓN ELECTRÓNICA.** (2014, julio). PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado a partir de https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WP4jIvk19ph

[35]. **RAY POYNTER.** (2012, noviembre). The Likert Scale. Recuperado a partir de http://thefutureplace.typepad.com/the_future_place/2010/09/the-likert-scale-tarsk-14-things-all-researchers-should-know.html

[36]. **SECURITY BY DEFAULT.** (2014, junio). SNMPDDOS:Exploiting SNMP for DDoS. Recuperado a partir de http://www.securitybydefault.com/2014/06/snmpddos-exploiting-snmp-for-ddos.html

[37]. **SMITH, R., MURTHY, S., GARCIA-LUNA-ACEVES, J.** (2011). Securing Distance-Vector Routing Protocols. *Symposium on Network and Distributed System Security*.

[38]. **SNMPDDOS: EXPLOITING SNMP FOR DDOS**. (s. f.). Recuperado a partir de http://www.securitybydefault.com/2014/06/snmpddos-exploiting-snmp-for-ddos.html

[39]. **SNORT.** (2011, Abril). Readme Filters. Recuperado a partir de https://www.snort.org/faq/readme-filters

[40]. **SNORT.** (2013). 3. Writing Snort Rules. Recuperado a partir de http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node27.html

[41]. **SPITZNER, L.** (2016). *Honeypots Tracking Hackers*. Addison-Wesley.

[42]. **UNAM MX.** (2005, junio). Monitoreo de Recursos de Red. Recuperado a partir de https://juliorestrepo.files.wordpress.com/2011/04/monitoreo.pdf

[43]. **US-CERT.** (2012, Enero). Denial of Service Attacks. Recuperado a partir de http://www.cert.org/information-for/denial_of_service.cfm

ANEXOS

ANEXO A. TABLA DE RESULTADOS

Objetivo: Conseguir el resultado para cada índice de la Variable Dependiente, utilizando las pruebas realizadas a las 3 amenazas (R. Puertos, F. Bruta, DDoS)

Prueba	Ataques				Prueba	Ataques				Prueba	Ataques			
1	dp	fb	ds	P	2	Dp	fb	ds	P	3	dp	fb	ds	P
Visual	1	1	1	1	visual	1	1	1	1	visual	1	1	1	1
Detec	5	5	5	5	detec	5	5	5	5	detec	5	5	5	5
Prevé	1	1	1	1	preve	1	1	1	1	preve	1	1	1	1

Prueba	Ataques				Prueba	Ataques				Prueba	Ataques				Prueba	Ataques			
4	dp	fb	ds	P	5	Dp	fb	ds	P	6	dp	fb	ds	P	7	dp	fb	ds	P
Visual	4	2	2	2,7	visual	4	2	2	2,7	visual	4	2	2	2,7	visual	4	2	2	2,7
Detec	5	5	5	5,0	detec	5	5	5	5,0	detec	5	5	5	5,0	detec	5	5	5	5,0
Prevé	5	5	5	5,0	preve	5	5	5	5,0	preve	5	5	5	5,0	preve	5	5	5	5,0

Prueba	Ataques				Prueba	Ataques				Prueba	Ataques				Prueba	Ataques			
8	dp	fb	ds	P	9	dp	fb	ds	P	10	dp	fb	ds	P	11	dp	fb	ds	P
Visual	4	4	1	3	visual	4	4	1	3	visual	4	4	1	3	visual	4	4	1	3
Detec	5	5	5	5	detec	5	5	5	5	detec	5	5	5	5	detec	5	5	5	5
Prevé	5	5	5	5	preve	5	5	5	5	preve	5	5	5	5	preve	5	5	5	5

Prueba	Ataques				Prueba	Ataques				Prueba	Ataques				Prueba	Ataques				Prueba	Ataques			
12	dp	fb	ds	P	13	dp	fb	ds	P	14	dp	fb	ds	P	15	dp	fb	ds	P	16	dp	fb	ds	P
Visual	4	4	1	3	visual	4	4	1	3	visual	4	4	1	3	visual	4	4	1	3	visual	4	4	1	3
Detec	5	5	5	5	detec	5	5	5	5	detec	5	5	5	5	detec	5	5	5	5	detec	5	5	5	5
Prevé	5	5	5	5	preve	5	5	5	5	preve	5	5	5	5	preve	5	5	5	5	preve	5	5	5	5

Prueba	Ataques			
17-30	dp	fb	ds	P
Visual	5	5	5	5
Detec	5	5	5	5
Prevé	5	5	5	5

#Pruebas		ÍNDICES			Observaciones
		Ingreso de ataque	Detección de ataque	Prevención de ataque	
prueba 1	día1	1	5	1	se realizan ataques, no detecta, no prev (config)
prueba 2	día2	1	5	1	se realizan ataques, no detecta, no prev (config)
prueba 3	día3	1	5	1	se realizan ataques, no detecta, no prev (config)
prueba 4	día4	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 5	día5	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 6	día6	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 7	día7	3	5	5	ingresa 1 ata, detecta 3 ata, prev 3
prueba 8	día8	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 9	día9	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 10	día10	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 11	día11	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 12	día12	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 13	día13	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 14	día14	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 15	día15	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 16	día16	3	5	5	ingresa 2 ata, detecta 3, prev 3 (no info web)
prueba 17	día17	5	5	5	ingresa, detecta, previene
prueba 18	día18	5	5	5	ingresa, detecta, previene
prueba 19	día19	5	5	5	ingresa, detecta, previene
prueba 20	día20	5	5	5	ingresa, detecta, previene
prueba 21	día21	5	5	5	ingresa, detecta, previene
prueba 22	día22	5	5	5	ingresa, detecta, previene
prueba 23	día23	5	5	5	ingresa, detecta, previene
prueba 24	día24	5	5	5	ingresa, detecta, previene
prueba 25	día25	5	5	5	ingresa, detecta, previene
prueba 26	día26	5	5	5	ingresa, detecta, previene
prueba 27	día27	5	5	5	ingresa, detecta, previene
prueba 28	día28	5	5	5	ingresa, detecta, previene
prueba 29	día29	5	5	5	ingresa, detecta, previene
prueba 30	día30	5	5	5	ingresa, detecta, previene
Total		119	150	138	
Likert		3,633333	5	4,5	

Interpretación de la tabla

Los 3 primeros días las pruebas no fueron satisfactorias ya que no se pudo visualizar ni detectar ni prevenir ningún ataque, por problemas de configuración.

Al 4to. día de pruebas se pudo detectar y prevenir los 3 ataques, pero solo se visualizó el ataque Rastreo de Puertos, hasta ese momento no se encontraba mucha documentación en internet sobre la forma correcta de instalación y configuración de Tshark en Centos y Wireshark en Ubuntu.

Al 8vo. día de pruebas, se logró instalar TShark 1.7.9 con lo que se visualizaron 2 ataques, Rastreo de Puertos y Fuerza Bruta, sin embargo se detectaron y previnieron los 3 ataques.

Al día 17 de pruebas y luego de una ardua investigación en internet, se decide desinstalar TShark 1.7.9 por la TShark 2.0.0 con la que se consigue visualizar, detectar y prevenir de forma correcta todos los ataques

Resultados

Luego de tabular todos los resultados, se calcula el total de todos índices, los mismos que para efecto de compararlos con la Escala de Likert, se los divide para la cantidad de pruebas realizadas, obteniendo la siguiente interpretación:

Escala Likert para ingreso de ataques=Total de Ingreso de ataques /total de Pruebas

109/30=3.63 [Mas o menos se detectaron los ataques]

Escala Likert para detección de ataques= Total de Detección de ataques/total de Pruebas

135/30=4,5 [Si cumple con la Detección de Ataques]

Escala Likert para prevención de ataques= Total de Prevención de ataques/total de Pruebas

135/30=4,5 [Si cumple con la Prevención de Ataques]

ANEXOS B. ESCALA DE COMPORTAMIENTO LIKERT

Escala de comportamiento tipo Likert. Dicha escala, a diferencia de las preguntas más usadas con respuestas de SI/NO, la escala de Likert nos permite medir actitudes y conocer el grado de conformidad del encuestado con cualquier afirmación que le propongamos ya que resulta especialmente útil emplearla en situaciones en que se desea matizar la opinión del encuestado. En este sentido, las categorías de respuestas, servirán para capturar la intensidad del individuo encuestado hacia dicha afirmación.

Escala de comportamiento tipo LIKERT	
1	**Fracaso**
2	**Insatisfactorio**
3	**Medianamente satisfactorio**
4	**Satisfactorio**
5	**Exitoso**

ANEXOS C. CATEGORIZACION DE REGLAS O FIRMAS EN SNORT

Classtype	Description	Priority
attempted-admin	Attempted Administrator Privilege Gain	high
attempted-user	Attempted User Privilege Gain	high
inappropriate-content	Inappropriate Content was Detected	high
policy-violation	Potential Corporate Privacy Violation	high
shellcode-detect	Executable code was detected	high
successful-admin	Successful Administrator Privilege Gain	high
successful-user	Successful User Privilege Gain	high
trojan-activity	A Network Trojan was detected	high
unsuccessful-user	Unsuccessful User Privilege Gain	high
web-application-attack	Web Application Attack	high
attempted-dos	Attempted Denial of Service	medium
attempted-recon	Attempted Information Leak	medium
bad-unknown	Potentially Bad Traffic	medium
default-login-attempt	Attempt to login by a default username and password	medium
denial-of-service	Detection of a Denial of Service Attack	medium
misc-attack	Misc Attack	medium
non-standard-protocol	Detection of a non-standard protocol or event	medium
rpc-portmap-decode	Decode of an RPC Query	medium
successful-dos	Denial of Service	medium
successful-recon-largescale	Large Scale Information Leak	medium
successful-recon-limited	Information Leak	medium
suspicious-filename-detect	A suspicious filename was detected	medium
suspicious-login	An attempted login using a suspicious username was detected	medium
system-call-detect	A system call was detected	medium
unusual-client-port-connection	A client was using an unusual port	medium
web-application-activity	Access to a potentially vulnerable web application	medium
icmp-event	Generic ICMP event	low
misc-activity	Misc activity	low
network-scan	Detection of a Network Scan	low
not-suspicious	Not Suspicious Traffic	low
protocol-command-decode	Generic Protocol Command Decode	low
string-detect	A suspicious string was detected	low
unknown	Unknown Traffic	low
tcp-connection	A TCP connection was detected	very low

Revisado por:

Director de Tesis: Ing. Vinicio Ramos Valencia, MIR